DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
Office of Information Services (OIS)
Security and Standards Group (SSG)
7500 Security Blvd
Baltimore, MD 21244-1850

CMS Information Systems Security Policy, Standards and Guidelines Handbook

(*The Handbook*)

Version 1.2

July 19, 2004

This page is intentionally left blank

Summary of changes in the Handbook version 1.2

1. **Section 13.3:** the note in the following section contained typographical errors and should read as the following:

Note: Use of the Internet is prohibited for health care transactions (claims, remittances, etc.) between Medicare carriers/intermediaries and providers. This Internet prohibition also applies to the transport of CMS Privacy Act-protected data between carriers/intermediaries and any other party. See the CMS Internet Security Policy for a definition of protected data at http://cms.hhs.gov/it/security, and Program Memoranda AB-01-11 (CR 1439) http://cms.hhs.gov/manuals/pm_trans/AB0111.pdf and AB-01-85 (CR 1749) http://www.cms.hhs.gov/manuals/pm_trans/A0185.pdf for this Internet prohibition.

Summary of changes in the Handbook version 1.1

2. **Section 1.2:** the following text was added to the end of the section:

"Article 35 of the 2004 Master Labor Agreement (MLA) defines "Computer Security and Personal Use of Agency Equipment and Resources." The Parties (CMS and the American Federation of Government Employees, AFGE, AFL-CIO) recognize that the Agency uses computer systems that contain sensitive information to accomplish its mission and that the Agency has a responsibility to ensure the security and privacy of such sensitive information. The Parties recognize the need to establish rules governing employees' acceptable use of Agency-owned or leased equipment and resources, including Internet addresses or domain names registered to the Agency."

3. **Section 2.2.18:** Sections 4-8 of the 2004 MLA were added to the Users Responsibilities

.

4. **Section 5.4:** Section 3 of the 2004 MLA was added to the CMS Training Program language.

5. **Appendix B:** Section 2 definitions from the 2004 MLA were added to the Glossary

    a. Agency-owned or Leased Equipment or Resources (NEW)
    b. Computer System (APPENDED)
    c. Sensitive Information (APPENDED)

CONTENTS

TABLES AND FIGURES

CHAPTER 1 - INTRODUCTION

1.1 Overview

The Centers for Medicare & Medicaid Services (CMS) is a Federal agency within the U.S. Department of Health and Human Services that administers the Medicare, Medicaid, and Child Health Insurance Programs. The success of CMS's mission "We assure health care security for beneficiaries" is reliant on an effective system security program to provide protection for beneficiary information. The CMS's system security mission ensures the existence of adequate safeguards to protect the personal, proprietary, and other sensitive data contained in its automated systems and protects the confidentiality, integrity, and availability of its information. CMS has recognized the need for increased security to ensure continuity of service for all business processes. Security program management and related implementation of controls over access to data, systems, and software programs are central factors affecting CMS's ability to protect its information resources.

This *CMS Information Systems Security Policy, Standards and Guidelines Handbook*, herein referred to as *The Handbook*, provides policy, standards and guidelines for administering the CMS Automated Information Systems (AIS) Security Program. This program is designed to protect CMS's internal and external information resources. The policies promulgated in the CMS AIS Security Program apply to all CMS organizations, employees, and contractors, or any other individuals who use CMS systems, data, or information. This program applies to all AIS, including the infrastructure and application environment.

1.2 Requirements

CMS's systems security requirements are based on external mandates such as the Privacy Act of 1974; Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources; the Computer Security Act of 1987; and the Department of Health and Human Services (DHHS), Information Resources Management (IRM) Circular No. 10, AIS Security Program.

The Privacy Act of 1974 requires federal agencies to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

OMB Circular A-130 requires agencies to establish a level of security for all agency information systems commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information systems. Appendix III of the circular mandates agencies shall ensure an adequate level of security for all agency automated systems, whether maintained in-house or commercially. It further specifies that agencies shall implement and

maintain an AIS security program, including the preparation of policies, standards, and procedures.

The Computer Security Act requires each federal agency to identify each computer system, whether operating or under development, within or under the supervision of that agency, which contains sensitive information. It also requires that each federal agency establish a plan for security and privacy of each computer system, within or under the supervision of that agency, which contains sensitive information. It further requires that each federal agency provide mandatory periodic training in computer systems security awareness and accepted computer systems security practices for all employees who are involved in the management, use, or operation of a computer system, within or under the supervision of that agency.

In accordance with Article 35 of the 2004 Master Labor Agreement (MLA), Computer Security and Personal Use of Agency Equipment and Resources, "The Parties (CMS and the American Federation of Government Employees, AFGE, AFL-CIO) recognize that the Agency uses computer systems that contain sensitive information to accomplish its mission and that the Agency has a responsibility to ensure the security and privacy of such sensitive information. The Parties recognize the need to establish rules governing employees' acceptable use of Agency-owned or leased equipment and resources, including Internet addresses or domain names registered to the Agency."

1.3 Scope

The Handbook is the policy document for the CMS AIS Security Program. It serves as the primary source of Information Technology (IT) systems security information for all CMS IT users. The policies, standards and guidelines described therein apply to all users of CMS hardware, software, information, and data. The CMS AIS Security Program ensures the existence of adequate safeguards to protect personal, proprietary, and other sensitive data in automated systems and ensures the physical protection of all CMS General Support Systems (GSSs) and Major Applications (MAs) that maintain and process sensitive data.

CHAPTER 2 - RESPONSIBILITIES

2.1 Overview

This chapter of *The Handbook* outlines and identifies responsibilities associated with the CMS AIS Security Program. The duties and responsibilities outlined in *The Handbook* may be delegated in writing by the office of primary responsibility or by the CMS Administrator.

The following individual responsibilities do not relieve the organizational components where the positions are located from complying with the system security requirements, including oversight of personnel assigned to the positions, since security is a management responsibility as well.

2.2 Responsibilities

2.2.1 CMS Administrator

The CMS Administrator has the overall responsibility for the implementation of an agency-wide Systems Security Program as directed by the DHHS, and for ensuring compliance with all legal requirements.

2.2.2 CMS Chief Information Officer

The CMS Chief Information Officer (CIO) is responsible for the implementation and administration of the CMS AIS Security Program. The CIO also has the responsibility to:

- Develop and implement policies, standards, guidelines and procedures that are consistent with DHHS and government-wide security policies, standards, and procedures to include those issued by the OMB, the Office of Personnel Management (OPM), and the National Institute of Standards and Technology (NIST).

- Implement and maintain an AIS Security Program to ensure that adequate security is provided for all information collected, processed, transmitted, stored, or disseminated in AIS to include MAs and GSSs.

- As the sole accrediting authority, determine the level of acceptable risk for all CMS information resources.

- Ensure there is an appropriate level of protection for all CMS information resources, whether retained in-house or under the control of contractors, including the establishment of physical, administrative, and technical safeguards.

2.2.3 Director, Office of Information Services

The Director, Office of Information Services (OIS) has overall responsibility for the CMS AIS Security Program. The Director, OIS also has the responsibility to:

- Establish systems security program requirements for CMS in compliance with DHHS AIS security policies.
- Provide leadership and focus to the CMS AIS Security Program.
- Provide resources necessary to administer CMS's AIS Security Program.
- Develop CMS's systems security budget.
- Develop overall CMS access control strategy for CMS's IT environment.
- Correct and monitor deficiencies identified by audits and evaluations.
- Appoint the CMS Senior Information Systems Security Officer.
- Ensure that appropriate systems security safeguards are in procurement requests.
- Evaluate safeguards used to protect major information systems.
- Determine MA and GSS designations based on CMS IT Architecture and NIST guidance.
- Perform official CMS AIS Security Program liaison activities with non-CMS government organizations and private organizations or committees, as required.
- Conduct information resources security awareness and training needs assessments, determine appropriate training resources, and coordinate training activities for target populations.

2.2.4 Director, Security and Standards Group

The Director, Security and Standards Group (SSG) has overall responsibility to administer the CMS AIS Security Program.

2.2.5 Senior Systems Security Advisor

The Senior Systems Security Advisor serves as principal advisor and technical authority to the CMS CIO and outside organizations on matters related to systems security.

2.2.6 Senior Information Systems Security Officer

The Senior Information Systems Security Officer (Senior ISSO) has the responsibility to:

- Evaluate and provide information about the CMS AIS Security Program to management and personnel, and communicate CMS AIS Security Program requirements and concerns.

- Ensure that System Security Plans (SSP) are developed, reviewed, implemented, and revised.

- Ensure that systems security risk assessments are developed, reviewed, and implemented for the SSP process.

- Report information resources security incidents in accordance with the systems security incident reporting procedures developed and implemented by federal mandates, DHHS, and CMS policies.

- Mediate and resolve systems security issues that arise between two CMS organizations, CMS and other federal organizations, or CMS and states or contractors.

- Maintain documentation used to establish systems security level designations for all SSPs within CMS.

- Assist component ISSOs in developing local systems security for either in place SSPs or for those under active development.

- Research state-of-the-art systems security technology and disseminate informational material in a timely fashion.

- Assure that ISSOs are appointed and trained.

- Develop and implement an AIS security training and orientation program in accordance with the requirements from the Computer Security Act of 1987.

2.2.7 Office/Center Directors/Regional Administrators

The CMS Office/Center Directors/Regional Administrators have the responsibility to:

- Ensure that their respective components are in compliance with the administrative, physical, and technical requirements of the CMS AIS Security Program.

- Designate Component ISSOs (Central and Regional Offices) (as appropriate), Application System, Database, Facilities, and other appropriate managers, and Resource Access Control Facility (RACF) Group Administrators within their components.

- Ensure that appropriate business continuity plans are developed, tested, and maintained within their organizations.

- Ensure a System Owner/Manager is appointed for each MA and a Database Manager is appointed for each database with a security level designation. (Temporary working files are excluded from this requirement.)

- Ensure personnel have received systems security awareness training.

2.2.8 Director, Investment Planning and Management Group

The Director of Investment Planning and Management Group (IPMG) has the responsibility to:

- Develop and maintain inventories of AIS systems and assets.

- Include systems security in the 5-year Information Resources Management (IRM) plan.

- Include systems security considerations in the IT Investment Review Board (ITIRB) investment decisions.

2.2.9 Group Directors/Division Directors

Group Directors/Division Directors have the responsibility to:

- Ensure their respective components are in compliance with the administrative, physical, and technical requirements of the CMS AIS Security Program.

- Ensure that personnel participate in system security awareness training.

- Develop and implement security requirements throughout the System Development Cycle (SDLC).

2.2.10 Component ISSOs (Central and Regional Offices)

Component ISSOs (Central and Regional Offices) have the responsibility to:

- Assist the CMS Senior ISSO in ensuring the component adheres to national systems security policies and procedures.

- Ensure component compliance with CMS's AIS Security Program requirements.

- Act on behalf of the component senior management in the assurance of systems security-related issues.

- Act as the primary point of contact in the component for information security issues.

- Act as a component focal point for the dissemination of systems security awareness information.

- Coordinate component reports on suspected systems security violations.
- Develop component systems security guidelines and procedures.
- Participate in the technical certification of component SSPs.
- Assist component with the development of SSPs during acquisition, development, and systems maintenance.
- Assist component with the development of business continuity plans during acquisition, development, and systems maintenance.
- Ensure component compliance with copyright laws and site licenses.
- Assist component in systems security matters in the SDLC process.
- Assist component RACF Group Administrators with systems security matters.
- Ensure audit trails are used where appropriate, in conjunction with System Owners/ Managers.

2.2.11 System Owners/Managers

System Owners/Managers have the responsibility to:

- Determine the sensitivity and criticality of the resources for which they are responsible.
- Define the system's functionality, configuration, and security requirements.
- Establish the rules for appropriate system use and protection of the subject data and information (rules of behavior) as required by the Privacy Act.
- Ensure a systems security risk assessment is prepared for each MA and GSS under their authority.
- Ensure a SSP is prepared for each MA and GSS under their authority.
- Officially certify and complete all required certification actions consistent with the CMS SSP Methodology.
- Implement the SSP and monitor its effectiveness.
- Develop the Business Continuity and Contingency Plan (BCCP).

2.2.12 System Maintainers/Developers

System Maintainers/Developers have the responsibility to develop and implement the security requirements throughout the SDLC at the same time System Owners/Managers define the requirements of the system. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for System Maintainers/Developers), or operational practices (e.g., awareness and training).

2.2.13 Database Administrators

Database Administrators have the responsibility to:

- Certify that systems security requirements of their databases are being met.
- Establish and communicate the security safeguards required for protecting databases based on the sensitivity levels of the data.
- Periodically review and verify that all users of their databases are authorized and are using the required systems security safeguards.

2.2.14 Resource Access Control Facility Administrator (RACF)

CMS's RACF Administrator is responsible for providing leadership and technical guidance in the use of RACF. The RACF Administrator has the responsibility to:

- Define the access control strategy for CMS enterprise security management.
- Implement resource access control with RACF for systems' data sets and resources.
- Assess system performance objectives related to RACF and tailor RACF to meet those objectives.
- Provide technical support in monitoring and reporting systems security related events.
- Provide support for implementing RACF interfaces with other major software program products and subsystems.

- Ensure all CMS components assign RACF Group Administrators for CMS groups and the contractor groups for which they are responsible.

- Provide RACF training to RACF Group Administrators.

2.2.15 RACF Group Administrators

The RACF Group Administrators are responsible for the implementation of RACF within their respective components. The RACF Group Administrator also has the responsibility to:

- Control user system access.

- Revoke system access to users when such action is appropriate.

- Define user, group, data set, and connect profiles as required to establish RACF protection for selected group performance.

- Modify component users or data set profiles to control RACF privileges and access to protected resources.

- Enter RACF commands that allow the desired level of user access to protected resources and monitor group performance.

- Assess systems security requirements of group-level data sets.

- Monitor the component's data sets to ensure proper protection of sensitive data.

- Assist users in their assessment of user-identification-level data sets.

- Provide RACF training to component personnel.

- Liaison with CMS operations support on RACF questions or problems for their component.

- Assist users in determining proper level of protection.

- Reset user passwords when users forget them.

- Maintain a common area for RACF general resource materials (manuals, reference cards, etc.).

2.2.16 Physical Security Officer

The Physical Security Officer (PSO) has the responsibility to:

- Ensure physical security of all hardware, software, and information stored and processed in CMS facilities.
- Ensure physical access control services are provided for all facilities.
- Ensure that all facilities fully comply with physical security requirements specified in CMS's AIS Security Program Handbook and DHHS security guidelines.
- Coordinate with management to determine the level of physical security required for facilities based on the sensitivity of the information being processed.
- Specify, implement, and review procedures used to protect the physical integrity of facilities and operating systems.
- Ensure that the physical security needs of all facilities are identified, incidents are monitored, and corrective actions are taken.
- Conduct risk analyses of all facilities to determine cost-effective and essential physical security safeguards.
- Ensure that all appropriate managers and users of all facilities are aware of the level of physical secure service offered, including safeguards that may be implemented and waivers received.
- Develop and maintain facility contingency plans, including the designation of personnel to be responsible for affecting backup operations in the event of major disruptions.
- Work with Project Officers, Contracting Officers, and ISSOs to ensure that Requests for Proposals (RFPs) pertaining to their facilities comply with physical security provisions of CMS's AIS Security Program in addition to participating in the technical review of proposals.
- Ensure that employees under his/her jurisdiction receive appropriate systems security training.

2.2.17 Supervisors

Supervisors at all levels have the responsibility to:

- Authorize employees' appropriate access to job-related resources.
- Ensure strict compliance with all legal requirements concerning the use of proprietary software (e.g., respecting copyrights and obtaining site licenses).
- Provide timely notification of all employee access revocations.

- Ensure that their employees are aware of, and comply with, all of the systems security requirements contained in the CMS AIS Security Program.

- Ensure that employees are aware of privacy and confidentiality requirements.

2.2.18 Users

Users have the responsibility to:

- Ensure the protection of CMS's hardware, software, information, and data by complying with the systems security requirements maintained in CMS AIS Security Program.

- Attend required computer systems security and functional training.

- Run application systems and databases only in authorized locations that are certified at a level of systems security equal to or higher than the security level designated for their application systems and databases.

- Ensure the protection of the privacy and confidentiality of all CMS data.

- Ensure confidentiality of their password.

In addition, CMS employees have the following responsibilities as listed in Article 35 of the 2004 MLA:

- "Employee users of Agency-owned or leased equipment and resources do not have an expectation of privacy while using such equipment or resources at any time, including times of permitted personal usage as set forth in Article 35 of the 2004 MLA. To the extent that employees desire to protect their privacy, employees should not use Agency-owned or leased equipment and resources. "

- "Use of Agency-owned or leased equipment and resources to accomplish work-related responsibilities will always have priority over personal use. In order to avoid capacity problems and to reduce the susceptibility of Agency information technology resources to computer viruses and cyber attacks, employees shall comply with the following requirements:

    A Personal files obtained via the Internet may not be stored on individual PC hard drives or on local area network (LAN) file servers.

    B Official video and voice files may not be downloaded from the Internet except when they will be used to serve an approved Agency function.

    C Internet and E-Mail etiquette, customs and courtesies shall be followed when using Agency-owned or leased equipment or resources."

- Permitted use of agency equipment includes the following:

"Agency-owned or leased equipment and resources are for Agency use and not for personal use; however, limited personal use of Agency-owned or leased equipment and resources by employees during non-work hours (i.e., weekends, before and after working hours or during lunch periods) is considered to be a permitted use of Agency-owned or leased equipment and resources when the following conditions are met:

A. Such use involves minimal additional expense to the Agency;

B. Such use does not interfere with the mission or operation of the Agency;

C. Such use does not violate the Standards of Ethical Conduct for Employees of the Executive Branch;

D. Such use does not overburden any Agency information resources; and

E. Such use is not otherwise prohibited under this Article.

Prohibited or inappropriate use of Agency-owned or leased equipment or resources by an employee could result in the loss of use or limitations on the use of such equipment or resources, criminal penalties, financial liability for the cost of inappropriate use or any other action deemed appropriate by the Agency."

- Prohibited usage of Agency Equipment and Resources

  "The following uses of Agency-owned or leased equipment or resources, either during working or non-working hours, are strictly prohibited:

  A. Activities that would compromise the security of any Government host computer. This includes, but is not limited to, sharing or disclosing log-in identification and passwords;

  B. Activities that would compromise the security of any Government host computer. This includes, but is not limited to, sharing or disclosing log-in identification and passwords;

  C. Fund-raising or partisan political activities, endorsements of any products or services or participation in any lobbying activity; or

  D. All E-mail communications to groups of employees that are subject to approval prior to distribution and have not been approved by the Agency (e.g., retirement announcements, Union notices or announcements, charitable solicitations)."

- General Internet and E-Mail requirements include the following:

A "Agency Internet and E-mail resources are the property of the Agency. Any use of Agency Internet and E-mail resources is made with the understanding that such use is not secure, private or anonymous.

B Employees using the Agency's Internet and E-mail resources are subject to having activities monitored by system or security personnel without any further specific notice.

C Employees should be aware that when they access the Internet using Internet addresses and domain names registered to the Agency, they may be perceived by others to represent the Agency. Employees shall not use the Internet for any purpose, which would reflect negatively on the Agency or its employees."

2.2.19 Procurement Contracting Officers

Contracting Officers are responsible for taking the following actions on procurements that involve the development of an AIS or the use of Federal Information Processing Standard (FIPS) resources:

- Ensure that the technical evaluation reports on successful proposals developed by the Project Officer either detail any AIS security deficiencies, or confirms contractor compliance with requirements.

- Ensure that the Pre-Award Certification statements of AIS security requirements for successful proposals are signed by both the Project Officer and the appropriate ISSO and are submitted with the proposals. The Contracting Officer is prohibited from initiating action on a proposal until a properly executed certification statement is received.

- Include a statement in the RFP requiring offerors to present a detailed outline of their proposed AIS security program in their proposals.

- Include a statement in the RFP that offerors are required to comply with the Statement of Work (SOW) and with the requirements of the CMS AIS Security Program. The statement must read substantially as follows:

    o *The contractor agrees to comply with the AIS security requirements set forth in the Statement of Work and applicable portions of the CMS AIS Security Program Handbook. The contractor further agrees to include this provision in any subcontract awarded pursuant to the prime contract. The contractor agrees to pay the costs of required security background investigations.*

- Forward to the appropriate component ISSO any forms that the winning contractor must submit to verify or obtain personnel security background investigations for the contractor's staff. If the winning contractor's personnel have not undergone required

background investigations, the awarding organization is responsible for assisting the contractor in obtaining the investigations. When it is necessary to begin contract work without the appropriate investigations, contractor personnel may begin parts of the work that are not sensitive. They must be closely monitored until investigations have been completed; if approval cannot be obtained, contractor personnel must be replaced. If a waiver is necessary, contact the Agency Personnel Security Representative (PSR).

- Furnish copies of *The Handbook* when requested by offerors who respond to the RFP.

2.2.20 Contractors

All contractors, subcontractors, and their employees supporting CMS are required to comply with the security requirements of the CMS AIS Security Program and all systems security related federal statutes, regulations, and policies.

2.2.21 Project Officers

Project Officers have the responsibility to:

- Authorize contractors and contractor employees appropriate access to job-related resources.

- Provide timely notification of all contractor and contractor employees' access revocations including notifying the CMS RACF Administrator for revocation of computer/data access and retrieval of badges and parking permits.

- Ensure that their contractor and contractor employees are aware of, and comply with, all of the systems security requirements contained in the CMS AIS Security Program.

2.2.22 Records Management

Records Management personnel are responsible for providing consultation to Database Managers to ensure that records retention schedules are adopted in accordance with CMS and DHHS guidance and that records disposal procedures are undertaken in accordance with the sensitivity of the data, including:

- Maintain CMS's Records Schedule, as approved by the National Archives and Records Administration, which provides a description of and disposition instructions for all files maintained by CMS and their contracts.

- Obtain Departmental, Office of General Counsel (OGC), and the Archivists' approval before revising CMS's Records Schedule.

- Oversee the storage and transfer of eligible CMS records at a federal storage facility.

- Conduct a file survey, the physical inspection of file areas and records management practices, and recommend improvements to those practices.

2.2.23 Freedom of Information Officer

The Freedom of Information Officer is responsible for implementing government guidelines and procedures so that information may be provided to meet requests made under the Privacy Act and the Freedom of Information Act (FOIA).

Automated systems of records subject to the Privacy Act containing information that meets the qualifications for Exemption 6 of the FOIA (i.e., for which unauthorized disclosure would constitute a “clearly unwarranted invasion of personal privacy” likely to lead to specific detrimental consequences for the individual in terms of financial, employment, medical, psychological, or social standing) must be adequately protected.

2.2.24 Privacy Officer

The Privacy Officer is the principal authority on maintenance and release of Privacy Act protected data from the Privacy Act System of Records (SOR). The Privacy Officer has the responsibility to:

- Interpret Privacy Act requirements and rules.

- Coordinate with all System Owners/Managers to ensure that they understand the Privacy Act requirements and their related responsibilities.

- Review requests and concur with the need to establish a new Privacy Act SOR or to modify an existing Privacy Act SOR.

- Assist System Owners/Managers in preparing Privacy Act SORs in accordance with established procedures.

- Ensure that SORs comply with the Privacy Act.

2.2.25 Human Resources Management Group (HRMG)

The HRMG determines the appropriate position sensitivity designations for critical and sensitive personnel positions, and ensures that employees have undergone appropriate background investigations.

CHAPTER 3 - SEPARATION OF DUTIES

3.1 Overview

This chapter of *The Handbook* applies to those individuals developing, implementing, operating, and maintaining CMS's automated information systems. It establishes CMS's policy at the highest level for separation of duties of those individuals. This policy helps to ensure that the inadvertent or deliberate corruption of CMS data assets does not occur.

3.2 Responsibilities

3.2.1 CMS Administrator

The CMS Administrator must stress consistently and regularly to CMS senior management the importance of separation of duties in managing CMS's automated information systems.

3.2.2 CMS Senior Management and Regional Administrators

CMS Senior Management and Regional Administrators have the responsibility to:

- Implement the Separation of Duties policy in a manner consistent with the policy, but tailored to their respective component and regional office environments.
- Ensure that it remains in effect, once adapted to their environments.

3.2.3 CMS CIO

The CMS CIO is responsible for promulgating the Separation of Duties policy across the agency and ensuring compliance.

3.2.4 Senior ISSO

The Senior ISSO shall establish the Separation of Duties policy and inform CMS Senior Management in Central Office and the Regions of any revisions or changes.

3.2.5 Policy

Each individual's duties within CMS's automated information systems environment shall be limited to duties that do not allow intentional or inadvertent unauthorized activity. All IT positions shall be subject to this policy and as such are prohibited from performing conflicting or incompatible duties. Examples of prohibited duties include but are not limited to simultaneous, concurrent, and multiple access rights for programming, application development, and operations functions during design, coding, testing and/or production.

This policy shall be included in all system security awareness and training programs for all CMS personnel.

3.3 References

3.3.1 Laws and Regulations

- *Computer Security Act of 1987* (Public Law 100-235). (1988).
- *Privacy Act of 1974* (Public Law 93-579, 5 U.S. Code 552a). (1974).
- *Training Requirement for the Computer Security Act* (Office of Personnel Management Regulation, 5 CFR Part 930).

3.3.2 Office of Management and Budget

- *Management of Federal Information Resources* (OMB Circular A-130, Appendix III, Security of Federal AIS). (February 8, 1996).

3.3.3 National Institute of Standards and Technology

- *Executive Guide to the Protection of Information Resources* (Special Publication No. 500-169). (October 1989).
- Management Guide to the Protection of Information Resources (Special Publication No. 500-170). (October 1989).

3.3.4 Department of Health and Human Services

- AIS Security Training and Orientation Program Guide (AIS-STOP). (November 1991).

CHAPTER 4 - PERSONNEL SECURITY/SUITABILITY

4.1 Overview

Every position within CMS, including those occupied by contractors, must be designated with a sensitivity level. All employees and contractors must meet personnel security/suitability standards commensurate with their position sensitivity level and are subject to personnel investigation requirements. Access to sensitive information is granted on demonstration of a valid need to know and not merely based on position, title, level of investigation conducted, or position-sensitivity level.

This chapter of *The Handbook* contains procedures and guidance for CMS's AIS Security Program Handbook derived from Circular A-130 (Revised), *Management of Federal Information Resources*, Appendix III; DHHS Personnel Instruction 731-1, *Personnel Security/Suitability Handbook*; and other federal guidelines. This chapter of *The Handbook* covers personnel security and suitability policy and procedures, including the designation of public-trust and sensitive positions, the scheduling and adjudication of personnel investigations, and the granting of access to sensitive information.

4.2 Responsibilities

4.2.1 CMS Management

CMS Management has the responsibility to:

- Determine the sensitivity level of all positions within their areas of responsibility and ensure that required background investigations are conducted.
- Establish effective methods for ensuring that consistent, timely, and equitable adjudicative determinations are made on all personnel security suitability cases involving their employees and contractors.
- Refer sensitive matters to the proper authorities for evaluation, investigation, or both.

4.2.2 The Director of Human Resources

The Director of Human Resources (DHR) has the responsibility to:

- Designate an official to serve as the Personnel Security Representative (PSR) to handle those responsibilities listed in the CMS AIS Security Program.
- Oversee, evaluate, and implement CMS's personnel security/suitability policies and programs.

4.2.2.1 The Division of Legal and Technical Services

Under the general direction of the DHR, the Division of Legal and Technical Services (DLTS) has the responsibility to:

- Develop, implement, and evaluate personnel security/suitability policies and programs.
- Provide program improvement recommendations through periodic assistance and evaluation visits to CMS components to ensure compliance to responsibilities regarding personnel security and suitability.
- Provide consultation, advice and guidance relating to personnel security and suitability policies and issues.
- Establish and maintain personnel security files for all employees and contractors.
- Request personnel investigations from OPM when required for employees and contractors in sensitive positions.
- Request and process personnel investigations of employees and contractor in sensitive positions.

4.2.2.2 Personnel Security Representative

The PSR has the responsibility to:

- Ensure that appropriate position sensitivity levels are designated for all positions.
- Adjudicate reports of investigation provided by OPM and delegate the adjudication responsibilities to the Servicing Personnel Officer (SPO**)** or other designated officials.
- Notify DHR when employees or contractors in public trust leave CMS.
- Ensure that top management officials are kept informed of pertinent personnel security and suitability matters and coordinate actions with the SPOs.
- Refer to the Director DLTS any developed unfavorable personnel security and suitability information on an employee, applicant, or contractor being considered for or occupying a sensitive or public-trust position.
- Submit to the CMS Director DLTS request for personnel investigation, waivers for personnel investigation and provide personnel security suitability data and reports.
- Forward of certification of investigation notice and any approved waiver request to the appropriate authorities.

- Ensure that each employee and contractor granted security access receives a security briefing or debriefing as appropriate.

4.2.2.3 Personnel Officer

The Personnel Officer has the responsibility to:

- Ensure that investigative requirements for each position are met and that any required waiver has been approved.

- Refer unfavorable personnel security and suitability information to the appropriate PSR, and coordinate actions with the office supervisor, OGC attorney, and Director DLTS, as necessary.

- Adjudicate National Agency Check (NAC) and National Agency Check and Inquiries (NACI) reports of investigation on individuals in sensitive or public-trust positions, or handling other adjudication responsibilities delegated by the PSR.

- Ensure that complete personnel security information is available to justify a decision concerning employment of personnel resigning from another federal agency.

4.2.3 Supervisors

Front Line Supervisors have the responsibility to:

- Ensure that employees promptly submit any required investigative forms to the appropriate PSR or SPO.

- Promptly provide the appropriate PSR or SPO with any unfavorable information regarding the conduct or behavior of a subordinate that indicates possible suitability or security concerns.

- Ensure that positions under their review are designated at the proper sensitivity level.

4.3 Position Sensitivity and Risk Designation - Guidance and Procedures

There are three position sensitivity designations (non-sensitive, public trust, and national security) which correlate with six specific sensitivity levels (Levels 1 through 6). CMS does not have any national security positions, therefore that position sensitivity and risk designation will not be detailed in this document. Determining whether a position has specific public-trust responsibilities is the key to designating the sensitivity level. Public-trust positions are designated as either Level 5 or 6. Without these special responsibilities, positions are designated as non-sensitive, which is Level 1 (see below).

4.3.1 AIS Public-Trust Positions

Generally, any federal service or contractor position in which the incumbent programs or operates a mainframe computer, or any other computer linked to others to form an AIS that allows for data access or manipulation, is a computer-related or AIS position. Positions requiring the use of a Personal Computer (PC) or word processor solely for composing correspondence with no linkage to an AIS or a network are not considered to be computer-related positions.

There are three position risk-level designations for AIS public-trust positions (high, moderate, and low risk) that correlate with specific sensitivity level. Determining whether a position has specific responsibility is the key to designating its sensitivity level. This is because public-trust positions are automatically designated at one of two levels (5 and 6). Position risk Levels 5 and 6 apply to most AIS positions. CMS management must decide which positions have these enhanced public-trust responsibilities and thus must be designated as public-trust positions. Management must further decide on the relative degree of risk, inherent in public-trust positions, so that they can assign a designated sensitivity level of high, moderate, or low. To promote consistency, effectiveness, and ease of operation, personnel security and ethics program designations must be linked. The ethics program regulations require that employees in specific, designated positions file an annual financial disclosure report (Standard Form [SF] 278 or Office of Government Ethics [OGE] 450) to ensure confidence in the integrity of the federal government by demonstrating they are able to carry out their duties without compromising the public trust. Therefore, CMS must use the ethics program designation as their initial step in determining whether a position is a public-trust position. CMS will maintain a list of designated positions and review them annually to ensure that only positions that meet the strict filing criteria are included. Management makes the most important personnel security decision in deciding the relative risk level (high, moderate, or low).

The minimum personnel background investigation requirements for the position sensitivity levels at CMS are as follows:

Table 1. Background Investigation Requirements: High Sensitivity

Level	Description	Required Investigation
3 (Level 6 with OPM)	High-Sensitivity “Public-Trust Positions”	Single Scope Background Investigation (SSBI)
2 (Level 5 with OPM)	Moderate-Risk “Public-Trust Positions”	NAC and Limited Background Investigation (LBI)

- **High Risk** (Level 3) public-trust positions have a potential for **EXCEPTIONALLY SERIOUS IMPACT** on computer security of an MA or GSS. Positions could include those in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or can access a system during the operation or maintenance stages, with relatively high risk for causing grave damage or realizing significant personal gain.

- **Moderate Risk** (Level 2) public-trust positions have the potential for **MODERATE TO SERIOUS IMPACT** on computer security, involving duties of considerable importance with significant program responsibilities that affect large portions of a MA or GSS. These positions include those in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the high-risk level to ensure the integrity of the system.

4.3.2 Non-Sensitive Positions

Table 2. Background Investigation Requirements: Non-Sensitive

Level	Description	Required Investigation
1 (Level 1 with OPM)	Low-Risk Non-Sensitive "Public-Trust Positions"	NACI (Name and fingerprint checks and written inquiries)

Low Risk (non-sensitive; Level 1) public-trust positions have the potential for **LIMITED** impact on the computer security of an MA or GSS. This level includes all AIS positions not within one of the above two risk levels. The majority of CMS positions are non-sensitive (Level 1) because CMS's mission involves mostly non-sensitive low-risk and non-sensitive program responsibilities. After having considered sensitive and public-trust responsibilities, those remaining positions are considered non-sensitive.

4.3.3 Suitability Determinations

The "suitability" or "fitness" decision is arrived at by a process that involves a prescribed series of actions. For a description of the suitability determination process, please consult the CMS Personnel Handbook.

4.3.4 Investigation Requirements

The Director DHR and each PSR must ensure that the analysis of background investigative information, the subsequent suitability/security determination, and the handling of the investigative reports follow the requirements, criteria, and standards in 5 Code of Federal Regulations (CFR) Parts 731, 732, and 736 and in Executive Order 10450. All pertinent information obtained from investigative reports, personnel records, responses to written inquiries, medical fitness records, personal or subject interviews, or

any other sources, must be considered in reaching suitability/security determinations. For an in-depth description of the investigatory requirements, consult the CMS Personnel Handbook.

4.3.5 Facts

The subject of the investigation must complete information on the questionnaires. However, to avoid unnecessary delays in initiating investigations, sometimes it is necessary for the PSRs or the DHR staff to amend or complete certain items before forwarding the forms to OPM. OPM has created Form FIPC 391 (Certification of Amended Investigative Form), which must be completed by the person amending the questionnaire when the subject is unable to personally make the changes. Any changes or additions must be consistent with subject's wishes and intent. OPM has a list of critical items on the three investigative forms that must be amended only by the subject.

4.3.5.1 Special Agreement Checks

OPM can establish Special Agreement Checks (SACs) with CMS to conduct specific records checks on individuals who need them to meet higher sensitivity levels. For example, to meet the National Agency Check and Inquiries and Credit (NACIC) requirement if an individual is moving from a non-sensitive (Level 1) position to a moderate risk public trust (Level 5), a credit record check only can be requested. The SAC will consist of record checks only and requests for SAC agreements must be discussed with and approved by the Director DHR.

4.3.5.2 Waivers

Special circumstances may require immediate action to employ an applicant or move an employee into a position designated as sensitive (Level 3) or public trust (Level 6). There may not be enough time to complete the required pre-appointment investigation, so a request for a waiver of that requirement may be made. A comprehensive representation of this process may be found in the CMS Personnel Handbook.

4.3.6 Description of Investigation Types

For a description of the various investigation types, see Appendix B, Glossary of Terms and Definitions.

4.3.7 Security Briefings

PSRs must ensure that each employee and contractor who has been granted an access or a security clearance receive briefings on security matters. Briefers must be familiar with *The Handbook* and use it as a reference guide.

- Initial security briefings must be conducted to inform individuals of the inherent responsibilities and proper procedures for handling and safeguarding information.

The briefing must occur before the individual is given access to such information. At the completion of the initial security briefing, the employee or contractor is required to sign an Information Nondisclosure Agreement (SF 312), and it shall be forwarded to the Director DLTS for retention.

- Refresher briefings must be given on a regular basis by the PSR to all individuals who have security clearances. They must be briefed on their continuing responsibilities for safeguarding information and on any new security regulations or procedures. Refresher briefings may be oral, written, or electronic. PSRs must maintain records to show that this requirement was met.

- Security debriefings must be given to all individuals upon termination of their security clearances or access. They shall be advised of their continuing responsibility for protecting the information to which they had access. On completion of the debriefing, the formerly cleared individual must sign the bottom half of the SF 312 labeled “Security Debriefing Acknowledgment”, and a witness signs it. The SF 312 must be forwarded to the Director DHR for retention.

4.3.8 Access Terminations, Clearance Downgrades, and Denials

The PSR, in coordination with the immediate supervisor and the Director DHR may determine that a currently cleared individual no longer has a need for a security clearance or access. That determination is a discretionary one and the decision of the Director DHR is conclusive. On written notice to the individual, the PSR may administratively terminate or downgrade the security clearance and access in the manner prescribed in the CMS Personnel Handbook.

4.3.9 Safeguarding and Handling Investigative Reports

All CMS officials, including PSRs, who review or store investigative reports and related information, must have had a favorable determination based on a background investigation that meets their sensitivity level.

4.4 References

4.4.1 Laws and Regulations

- *Computer Security Act of 1987* (Public Law 100-235). (1988).

- *Privacy Act of 1974* (Public Law 93-579, 5 U.S. Code 552a). (1974).

- *Training Requirement for the Computer Security Act* (Office of Personnel Management Regulation, 5 CFR Parts 731, 732, 736, and 930).

- Executive Order 10450.

4.4.2 Office of Management and Budget

- *Management of Federal Information Resources* (OMB Circular A-130, Appendix III, Security of Federal AIS). (February 8, 1996).

4.4.3 National Institute of Standards and Technology

- *Executive Guide to the Protection of Information Resources* (Special Publication No. 500-169). (October 1989).
- *Management Guide to the Protection of Information Resources* (Special Publication No. 500-170). (October 1989).
- *Computer User's Guide to the Protection of Information Resources* (Special Publication No. 500-171). (December 1989).
- *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (NIST Publication No. 800-16).

4.4.4 Department of Health and Human Services

- *AIS Security Training and Orientation Program Guide* (AIS-STOP). (November 1991).
- *Personnel Security/Suitability Policy and Technical Guidance* (Personnel Manual, Instruction 731-1).
- *Supervisor's Guide to Personnel*.
- DHHS *Personnel Security/Suitability Handbook*.

CHAPTER 5 - SYSTEMS SECURITY AWARENESS, TRAINING, AND EDUCATION

5.1 Overview

CMS is committed to a comprehensive Systems Security Awareness, Training, and Education (SSATE) program for its employees, contractors and management to ensure compliance with federal security regulations. Federal agencies cannot protect the confidentiality, integrity, and availability of their information in today's highly networked systems environment without ensuring that each person involved understands their systems security role and responsibilities and is adequately trained to perform them. An effective SSATE is essential for the overall systems security program. Without knowing and understanding the necessary and appropriate security measures (and how to use them), users cannot be truly accountable for their actions.

5.2 Responsibilities

5.2.1 CMS Management

CMS Management (Office/Center Directors/Regional Administrators/Group Directors/Division Directors) is responsible to ensure personnel have received systems security awareness training and participate in technical security training sessions where appropriate.

5.2.2 Senior ISSO

The Senior ISSO has the responsibility to develop and implement an AIS security training and orientation program in accordance with the requirements of the Computer Security Act of 1987.

5.2.3 Component ISSOs (Central and Regional Offices)

Component ISSOs (Central and Regional Offices) have the responsibility to act as the point of contact for the dissemination of systems security awareness information.

5.3 Approach

The overall goal of a SSATE is to increase employee awareness of their computer systems security responsibilities and the ways to fulfill those responsibilities in order to sustain an appropriate level of protection for computer resources. CMS's approach for ensuring the protection of IT resources is based on training directed and tailored to individual employee needs, career mobility, and to CMS's evolving and changing mission. This approach will:

- Improve awareness of the need to protect system resources.
- Develop skills and knowledge so computer users can perform their jobs more securely.
- Build in-depth knowledge, as needed, to design, implement, or operate systems security programs for organizations and systems.

5.4 CMS Training Program

Public Law 100-235, the Computer Security Act of 1987, requires mandatory periodic training for all employees involved in the management or use of federal computer systems that contain sensitive information. OPM Regulation, 5 CFR Part 930, titled *Training Requirement for the Computer Security Act*, specifies the content, target populations, and training levels for the requirement. NIST Special Publication Number 500-172, *Computer Security Training Guidelines*, and the DHHS AIS-STOP provide guidance in meeting the requirement.

In compliance with the Computer Security Act of 1987 (P.L. 100-235), the Agency agrees to provide appropriate training to employees involved in the operation or use of computer systems containing sensitive information to enhance employees' awareness of the threats and vulnerabilities of computer systems and to encourage the use of improved security practices.

CMS uses different general levels of training that are appropriate for different target audiences. The training levels depend on the sensitivity and criticality of the information and the security responsibilities of the systems.
Systems security awareness and training is an on-going process needed to sustain a secure environment. Systems security awareness is included by CMS as part of its existing computer training, management courses, and new employee orientations. Delivery methods include classroom, computer-based training, videotapes, workbooks, job aids, and desk guides. Training areas include:

- **Computer Systems Security Basics:** basic principles and concepts of information as defined by industry standards and federal publications.
- **Computer Systems Security Policy and Procedures:** policy and procedures that are appropriate to CMS. These include all policy and procedures mandated by external government agencies such as OMB and NIST, as well as all appropriate internal material.
- **SSP Methodology:** the development, implementation, and maintenance of a viable SSP in support of CMS's stated mission.
- **Risk Assessment:** the ability to identify threats and vulnerabilities to systems within CMS in a cost-effective manner.

- **Operational Security:** the administration and maintenance of security features in software and administrative policy either developed or procured in support of all agency programs.

- **Network Computer Security Basics:** basic principles and concepts of information for networks as defined by industry standards and Federal publications.

5.5 References

5.5.1 Laws and Regulations

- *Computer Security Act of 1987* (Public Law 100-235). (1988).

- *Privacy Act of 1974* (Public Law 93-579, 5 U.S. Code 552a). (1974).

- *Training Requirement for the Computer Security Act* (Office of Personnel Management Regulation, 5 CFR Part 930).

5.5.2 Office of Management and Budget

- *Management of Federal Information Resources* (OMB Circular A-130, Appendix III, Security of Federal AIS). (February 8, 1986).

5.5.3 National Institute of Standards and Technology

- *Executive Guide to the Protection of Information Resources* (Special Publication No. 500-169). (October 1989).

- *Management Guide to the Protection of Information Resources* (Special Publication No. 500-170). (October 1989).

- *Computer User's Guide to the Protection of Information Resources* (Special Publication No. 500-171). (December 1989).

- *Information Technology security Training Requirements: A Role- and Performance-Based Model (*NIST Special Publication 800-016).

- NIST Training Matrix (NIST Special Publication 500-172).

5.5.4 Department of Health and Human Services

- *AIS Security Training and Orientation Program Guide (*AIS-STOP). (November 1991).

- *Computer Security for Senior Executives*. (June 11, 1993).

- *Microcomputer Security Training* (IRM Circular No. 18.). (December 27, 1992).

- *Personnel Security/Suitability Policy and Technical Guidance* (Personnel Manual, Instruction 731-1).

CHAPTER 6 - RISK MANAGEMENT

6.1 Overview

Risk management provides a disciplined environment for assessing what can go wrong in projects (both technically and managerially), determining the relative importance of identified risks, implementing strategies to deal with these risks, and focusing management's attention for effective, proactive, fact-based decision making. Risk management also provides a tool for analyzing the security costs and benefits of various contingency planning options. In addition, a risk management effort can be used to help identify critical resources needed to support an organization and the likely threat to those resources.

A CMS security risk assessment standard is under development. This chapter of *The Handbook* describes the basic elements of successful risk management and how it is instituted to ensure a continuous review of automated systems critical to its mission at the organizational level.

6.2 Responsibilities

6.2.1 CMS Management

CMS Management (Office/Center Directors/ Regional Administrators/Group Directors/Division Directors) has the responsibility to:

- Ensure that appropriate risk assessments covering all data, MAs, and GSSs under their jurisdiction are performed.
- Approve risk mitigation plans, risk prioritization, and the closure of risks.
- Facilitate timely actions and decisions.

6.2.2 Component ISSOs (Central and Regional Offices)

Component ISSOs (Central and Regional Offices) are responsible to participate with components to ensure that risk management is integrated into all GSSs and MAs.

6.2.3 System Owners/Managers

The System Owners/Managers have the responsibility to:

- Conduct regular risk assessment of GSSs and MAs to determine cost-effective and essential information system security safeguards.
- Develop and implement mitigation plans for those risks for which they have the authority to commit resources.

- Provide a copy of all system risk assessments to the System Maintainers/Developers as input for the development of SSPs.

- Maintain a copy of risk assessment reports for seven years.

6.3 Policy

CMS requires that all system and information owners develop, implement and maintain risk assessments to ensure that appropriate safeguards are taken to protect all CMS resources. A risk-based approach must be used to determine adequate security and must include a consideration of the major factors in management such as the value of the system or application, all threats, all vulnerabilities, and the effectiveness of current or proposed safeguards. Additional guidance on effective risk assessment can be found in *An Introduction to Computer Security: The NIST Handbook*.

6.4 Risk Assessment

The objective of a risk assessment is to determine the current level of risk associated with the implementation of a system. The risk assessment must be included with the SSP. First, the assets related to the system must be identified and valued. Then, specific threats and vulnerabilities are identified and analyzed for the possible losses that could be incurred. Next, potential safeguards are evaluated to select those that are most cost-effective in addressing the threats and eliminating or reducing the vulnerabilities to an acceptable level of risk.

System Owners/Managers and System Maintainers/Developers must conduct a risk assessment every year for a GSS or a high risk MA; every three years for all other MAs and “other systems”; whenever significant modifications are made to the system; or whenever a major security violation occurs. The System Owners/Managers must retain all risk assessment reports and supporting documentation for at least seven years.

A risk assessment consists of the following:

- Asset Valuation

- Threat Determination

- Vulnerability Identification

- Safeguard Analysis

- Safeguard Selection and Implementation

6.4.1 Asset Valuation

Asset values included in the risk assessment will be taken from information gathered from personnel, documentation, and other local sources during data collection visits or by use of industry-accepted asset estimation tools.

6.4.2 Threat Determination

Threat determination requires the identification and assessment of potential threats to CMS IT resources. Potential threats include both natural disasters and people who can disrupt operations, time dependent services, or can cause loss of physical assets, loss of system integrity, or harm to the business of the organization, whether intentional or unintentional. The risk assessment must result in a list of threats for every aspect of the sensitive GSS and/or MA.

6.4.3 Vulnerability Identification

Vulnerability identification involves the determination of weaknesses or flaws that exist in a sensitive system or facility that could allow a threat to affect its security. Vulnerability identification must be performed on new, existing, and recently modified sensitive systems and facilities. A summary list of vulnerabilities must be prepared for each sensitive system and facility being analyzed.

6.4.4 Safeguard Analysis

The next step includes the identification and assessment of possible safeguard measures and their related costs. The safeguards identified must fulfill the minimum-security safeguard requirements. One method of selecting safeguards uses a “what if” analysis. With this method, the effect of adding various safeguards (and thereby reducing vulnerabilities) is tested to see what difference each makes with regard to cost, effectiveness, and other relevant factors. Trade-offs among the factors can be seen. The analysis of trade-offs also supports the acceptance of residual risk. This method typically involves multiple iterations of the risk assessment to see how the proposed changes affect the risk assessment result. Another method is to categorize types of safeguards and recommend implementing them for various levels of risk. For example, stronger controls would be implemented on high-risk systems than on low-risk systems. This method normally does not require multiple iterations of the risk assessment. As with other aspects of risk management, screening can be used to concentrate on the highest-risk areas.

6.4.5 Safeguard Selection and Implementation

Based on the risk assessment, System Owners/Managers and System Maintainers/ Developers must select specific information system security safeguards that allow the greatest reduction in risk for the most reasonable cost. During this process, these managers must identify those safeguards that will protect multiple systems and facilities and those safeguards that may affect another system negatively.

6.5 References

6.5.1 National Institute of Standards and Technology

- *Introduction to Computer Security: The NIST Handbook* (October 1995).

6.5.2 Department of Health and Human Services

- *Automated Information Systems Security Program Handbook* (DHHS guide). (October 1995).

CHAPTER 7 - INTEGRATING COMPUTER SYSTEMS SECURITY INTO THE SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)

7.1 Overview

This chapter of *The Handbook* supports the development and maintenance of systems security throughout the SDLC by providing an overview of the CMS SDLC standard, and system security elements applicable to meeting that standard. CMS's approach for implementing systems security controls crosses organizational lines and uses SSPs to ensure systems security is considered during all phases of an IT system life cycle.

7.2 Responsibilities

7.2.1 Component ISSOs (Central and Regional Offices)

The Component ISSOs (Central and Regional Offices) in each CMS organization have the responsibility to:

- Assist System Owners/Managers in selecting and implementing appropriate administrative, physical, and technical safeguards for application systems under development or enhancement.
- Ensure component compliance with CMS’s AIS Security Program requirements.
- Act on behalf of the component senior management in the assurance of systems security-related issues.
- Participate in the technical certification of component SSPs.
- Assist component with the development of SSPs during acquisition, development, and systems maintenance.
- Assist component with the development of contingency plans during acquisition, development, and systems maintenance.
- Ensure component compliance with copyright laws and site licenses.
- Assist component in systems security matters in the SDLC process.
- Assist component RACF Group Administrators with systems security matters.
- Ensure audit trails are used where appropriate, in conjunction with System Owners/Managers.

7.2.2 System Owners/Managers

System Owners/Managers have the responsibility to:

- Assess and determine the sensitivity of the data in the system.
- Define the system's functionality, configuration, and security requirements.
- Establish the rules for appropriate system use and protection of the subject data and information (rules of behavior).
- Ensure that a security risk assessment is prepared for each MA and GSS under their authority.
- Ensure that appropriate administrative, physical, and technical safeguards, commensurate with the security level designation of the system, are incorporated into their application systems under development or enhancement.
- Ensure that a SSP is prepared for each MA and GSS under their authority.
- Implement the SSP and monitor its effectiveness.

7.3 Implementation of Systems Security in the SDLC

The implementation of an effective system security planning process begins at the start of the SDLC process and culminates with the retirement of a system. To understand the application of *The Handbook* to the system life cycle, one must first understand the CMS SDLC. A brief overview of the CMS SDLC is provided in the paragraphs below.

7.3.1 CMS SDLC Overview

The CMS SDLC is presented as three life-cycle phases and a series of activities that occur within each phase. The grouping of activities into three life-cycle phases is simply based on those activities that take place before development, those that take place during development, and those that take place after development. The three phases are:

- Pre-Development Phase
- Development Phase
- Post Development Phase.
- These life cycle phases and activities represent the series of activities that occur throughout a system's lifetime, from beginning to end. All of these activities occur in sequence within each life-cycle phase, but within the Development Phase, the sequence will usually be iterated several times depending on the development

strategy. For further explanation of CMS's SDLC, see the CMS System Development Life Cycle Standard.

7.3.2 System Security Life Cycle

The system security life cycle closely follows the SDLC. Each of the life-cycle phases is discussed below.

7.3.2.1 Pre-Development Phase

During the pre-development phase, the need for a system is expressed and the purpose of the system is documented. A determination on the sensitivity of the information to be processed and the system itself must be made. The sensitivity and criticality of the information stored within, processed by, or transmitted by the system provides the basis for the value of the system and is one of the major factors in risk management. An initial risk assessment must be prepared during this phase. System planners define the requirements for the system. Systems security requirements must also be developed at the same time. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for system maintainers/developers), or operational practices (e.g., awareness and training).

Note: Initiation of the SSP is based on available information at the onset of the SDLC process.

A sensitivity assessment must be completed which looks at the sensitivity of both the information to be processed and the system itself. The assessment must consider legal implications, organization policy (including federal and agency policy if a federal system), and the functional needs of the system. A sensitivity assessment must answer the following questions:

- What information is handled by the system?
- What kind of potential damage could occur through error, unauthorized disclosure or modification, or unavailability of data or the system?
- What laws or regulations affect systems security (e.g., the Privacy Act or the Fair Trade Practices Act)?
- To what threats is the system or information particularly vulnerable?
- Are there significant environmental considerations (e.g., hazardous location of system)?
- What are the systems security-relevant characteristics of the user community (e.g., level of technical sophistication and training or security clearances)?

- What internal systems security standards, regulations, or guidelines apply to this system?

- The sensitivity assessment starts an analysis of systems security that continues throughout the life cycle. The assessment helps determine if the project needs special systems security oversight, if further analysis is needed before committing to begin system development (to ensure feasibility at a reasonable cost), or in rare instances, whether the systems security requirements are so strenuous and costly that system development or acquisition will not be pursued (NIST *Introduction to Computer Security Handbook*, 800-12, 1995).

As part of the pre-development activities, the appropriate ISSO conducts an initial risk assessment to determine potential threats, identify vulnerabilities, estimate the magnitude of potential losses, and identify possible safeguards and related costs. A product of this activity is a preliminary risk assessment report that must be included in the Concept of Operations document. A complete risk assessment cannot be done at this stage of development but consideration of risk begins during the pre-development phase, and is updated and revised during subsequent phases.

After conducting the risk assessment, a cost-benefit analysis is done that examines the assets, threats, and vulnerabilities of the system to determine the most appropriate cost-effective safeguards. A cost-benefit analysis report that includes recommendations for cost-effective safeguards must be produced as part of the Concept of Operations document.

7.3.2.2 Development Phase

During the development phase, the system is designed, purchased, programmed, developed, or otherwise constructed. During this phase, the SSP must be functional as the phase approaches its end. Changes will continue to be made as the system matures and technology changes. Systems security questions that must be addressed include:

- During the system design, were systems security requirements identified?

- Were the appropriate systems security controls, with associated evaluation and test procedures, developed before the procurement action?

- Did the solicitation documents include systems security requirements and evaluations, test procedures, or both?

- Did the requirements permit updating systems security requirements as new threats and vulnerabilities are identified and as new technologies are implemented?

- Have additional risks identified during the development phase been reflected in the existing risk assessment and have plans addressed risk management? Have other

risks been mitigated by the development and if so, has the risk assessment been updated to reflect the change in risk management?

The system's security features must be configured and enabled, the system must be tested and installed or fielded, and the system must be authorized for processing. A design review and systems test must be performed before placing the system into operation to ensure that it meets systems security specifications. These activities support or coincide with the certification and accreditation activities all systems must undergo to ensure systems security compliance. System certification is typically performed by the System Owner/Manager and Systems Maintainer/Developer as a management control. Accreditation of a system must be performed by the CMS CIO or a senior management official designee. Furthermore, if new controls are added to the application or support system, additional acceptance tests of those new controls must be performed. This ensures that new controls meet systems security specifications and do not conflict with or invalidate existing controls. For further explanation, see the CMS SSP.

Note: At the end of this phase, the SSP must be complete and functional.

The development phase contains activities that proceed from requirements gathering and analysis and system design through coding to testing and acceptance.

7.3.2.3 Post Development Phase

During this phase, the system performs its work. If the system undergoes modifications, any changes to systems security activities must be documented in the SSP. These changes include level of risk, management of the risk, and mitigation or elimination of the existing risks. In the SSP, systems security operations and administration, operational assurance, and audits and monitoring must be described.

Note: During this phase of the SDLC, the SSP is the most complete and must be revised whenever there is a significant modification, a major security violation has occurred, or the certification and accreditation has expired.

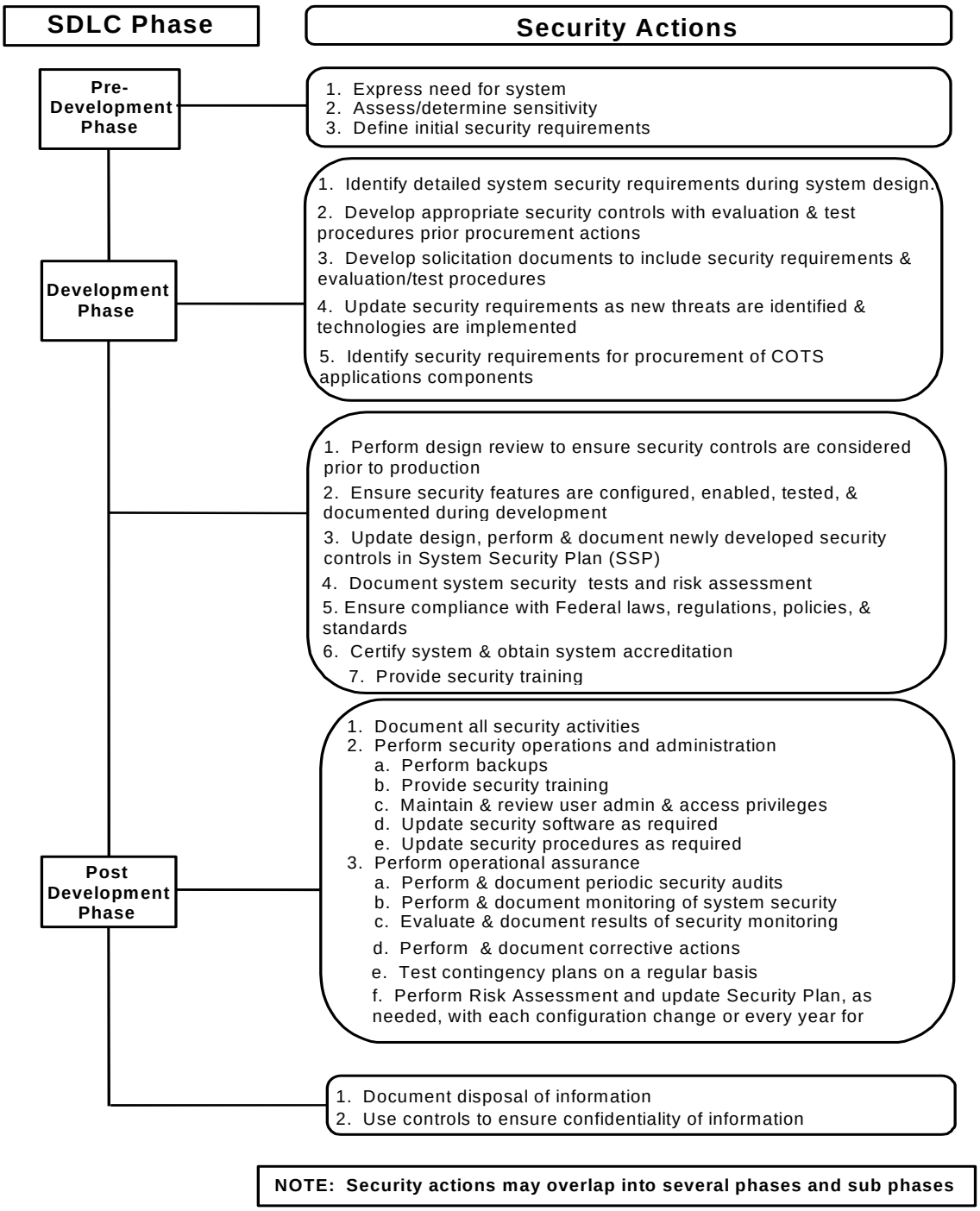
The end of this phase of the life cycle involves the disposition of information, hardware, and software when the system is at the completion of its use.

Note: At the completion of a systems life cycle (disposal of a system), the SSP must be archived.

7.3.3 Systems Security Activities Associated with the SDLC

Figure 1 graphically represents each of the SDLC phases with the specific systems security actions that need to occur during that phase of the SDLC.

Figure 1. SDLC Phases



7.4 References

7.4.1 Department of Health and Human Services

- *Automated Information Systems Security Program Handbook* (DHHS guide). (October 1995).

7.4.2 Centers for Medicare & Medicaid Services

- *CMS System Development Life Cycle Standard (Oct 7, 1999).*

7.4.3 Other

- *IEEE/EIA 12207.0*

CHAPTER 8 - INFORMATION SECURITY LEVEL DESIGNATIONS

8.1 Overview

The systems security efforts of the CMS AIS Security Program are based on the sensitivity of data contained in MAs and GSSs, and the operational criticality of the data processing capabilities of those systems. Security level designations are used to define the requirements of security efforts to protect CMS's information assets. Some of CMS's most critical information assets are the data recorded in these assets, such as financial, Medicare, patient, and hospital records.

8.2 Responsibilities

8.2.1 System Owners/Managers

System Owners/Managers have the responsibility to:

- Determine and document the data sensitivity and application criticality of the resources for which they are responsible.
- Identify appropriate security level designation for their systems.

8.2.2 System Maintainers/Developers

System Maintainers/Developers have the responsibility to implement the security requirements throughout the SDLC using the security level designation as the basis.

8.3 Information Security Levels

The security level designations within the CMS AIS Security Program are based on the following:

- The sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse).
- The operational criticality of data processing capabilities (i.e., the ramifications if data processing capabilities were interrupted for a period of time or subject to fraud or abuse).

There are four security level designations for data sensitivity and four security level designations for operational criticality. These security levels are summarized in Table 3 and described in more detail later in this chapter.

Table 3. Summary of Sensitivity and Criticality Levels

Level	Sensitivity	Criticality
1	Threats to this data are minimal and only minimal precautions to protect the data need to be taken. Unintentional alteration or destruction is the primary concern for this type of data.	Systems requiring minimal protection. In the event of alteration or failure, it would have a minimal impact or could be replaced with minimal staff time or expense. This includes data that has low or no sensitivity.
2	Data has importance to CMS and must be protected against such acts as malicious destruction. However, because this type of data is most often collected for analytical purposes, disclosure problems are not usually significant.	Systems that are important but not critical to the internal management of CMS. If systems fail to function for an extended period of time, it would not have a critical impact on the organizations they support. This includes data that has moderate sensitivity.
3	The most sensitive unclassified data (other than unclassified data whose loss could adversely affect national security interests). This data requires the greatest number and most stringent information security safeguards at the user level.	Systems that are critical to CMS. This includes systems whose failure to function for even a short period of time could have a severe impact or has a high potential for fraud, waste, or abuse. This includes data that has high sensitivity.
4	All databases that contain national security classified information and all databases that contain other sensitive but unclassified information, the loss of which could adversely affect national security interests. (CMS currently processes no information in this category.)	Systems are critical to the well-being of CMS such as systems that handle sensitive but unclassified information, the loss of which could adversely affect national security interests. These systems must be protected in proportion to the threat of compromise or exploitation and the associated potential damage.

The appropriate System Owner/Manager and System Maintainer/Developer must consider each system from both points of view, then choose the higher rating for the overall security level designation.

An MA or GSS may be compartmentalized, such that a given data set or sub-process is more sensitive than other data sets or sub-processes. The appropriate System Owner/Manager and System Maintainer/Developer must assign the highest security level designation of any data set or sub-process within the system for the overall security level designation. This practice supports the following:

- **Confidentiality.** The system contains information that requires protection from unauthorized disclosure.
- **Integrity.** The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification, including the detection of such activities.

- **Availability**. The system contains information or provides services that must be available on timely basis to meet mission requirements or to avoid substantial losses.

System Owners/Managers and System Maintainers/Developers must ensure that their databases and the processing capabilities of their systems are accessed only by authorized users who fully use the required security level safeguards. The managers of compartmentalized systems must take special care to specify the appropriate level of security required when negotiating with GSSs and MAs for services. The security level designation determines the minimum-security safeguards required to protect sensitive data and to ensure the operational continuity of critical data processing capabilities.

8.3.1 Sensitivity Levels for Data

Sensitivity levels are assigned to data based on the highest level of sensitivity of the data and the requirements of specific laws governing the protection or disclosure of information (e.g., the Privacy Act).

8.3.1.1 Level 1: Low Sensitivity

This category identifies data that requires minimal protection. Threats to this data are minimal, and only minimal precautions to protect the data need to be taken. Unintentional alteration or destruction is the primary concern for this type of data. This category includes the following:

- Data only in its raw form, such as in some laboratory research applications, and the computerized correspondence and documents in some offices.

- Automated Systems of Records, which contain information that is virtually in the public domain, such as employee locator files, and for which any unauthorized disclosures could be expected not to adversely affect the individual.

8.3.1.2 Level 2: Moderate Sensitivity

This category identifies data that has importance to CMS and which must be protected against such acts as malicious destruction. However, because this type of data is most often collected for analytical purposes, disclosure problems are not usually significant. This category includes the following:

- Management information concerning workload, performance, staffing, and similar data, usually in statistical form, is used to generate reports that reflect the status of an organization. Access to this data needs to be restricted only to a limited degree. The data is protected because of its value to the organization but is intended for disclosure in some form eventually.

- Research and statistical data accumulated to provide information about CMS programs to the public. This data needs protection commensurate with the value of

the information to the organization. Loss of this kind of data would not normally be potentially embarrassing or detrimental either to an individual or to the organization.

- Automated systems of records subject to the Privacy Act, which contain information not in the public domain, but for which unauthorized disclosure could cause nonspecific embarrassment to an individual.

- Computerized correspondence and documents, which must be protected from unauthorized alteration or disclosure. These types of data include all correspondence, memoranda, and other documents whose release or distribution outside the federal government or within the organization needs to be controlled.

8.3.1.3 Level 3: High Sensitivity

This category contains the most sensitive unclassified data (other than unclassified data whose loss could adversely affect national security interests). The data in this category requires the greatest number and most stringent information security safeguards at the user level. This category includes the following:

- Payment information that is used to authorize or make cash payments to individuals or organizations. This data is usually stored in production application files and systems, and includes benefit information, such as that found at the Social Security Administration, and payroll information. Such information also includes databases that the user has the authority and capability to use or alter to cause an improper payment.

- Proprietary information that has value in and of itself and that must be protected from unauthorized disclosure.

- Computerized correspondence and documents that are considered highly sensitive or critical to an organization and that must be protected from unauthorized alteration or premature disclosure.

- Automated systems of records subject to the Privacy Act, which contain information that meets the qualifications for Exemption 6 of the FOIA; that is, for which unauthorized disclosure would constitute a “clearly unwarranted invasion of personal privacy” likely to lead to specific detrimental consequences for the individual in terms of financial, employment, medical, psychological, or social standing.

8.3.1.4 Level 4: High Sensitivity and National Security Interest

CMS currently processes no information in this category. This category identifies all databases that contain national security classified information and all databases that contain other sensitive, but unclassified information, the loss of which could adversely affect national security interests.

8.3.2 Criticality Levels for Application Systems

Criticality levels are assigned to systems based upon the relative importance of their processing capabilities to the organizations they support. A Level 1 designation is used for a system with the lowest criticality of data processing relative to the organization it supports; and a Level 4 designation is used for a system with the highest criticality.

8.3.2.1 Level 1: Low Criticality

This category identifies systems with data processing capabilities that require minimal protection. -These include systems that, in the event of alteration or failure, would affect the organization minimally or could be replaced with minimal staff time or expense. This category also includes systems that generate, store, process, transfer, or communicate data that is considered to have low or no sensitivity (Level 1).

8.3.2.2 Level 2: Moderate Criticality

This category identifies systems with data processing capabilities that are considered important but not critical to the internal management of CMS. This category includes the following:

- Systems in which failure to function for an extended period of time would not have a critical impact on the organizations they support.

- Systems that generate, store, process, transfer, or communicate data that are considered to have moderate sensitivity (Level 2).

8.3.2.3 Level 3: High Criticality

This category identifies systems with data processing capabilities that are considered critical to CMS. This category includes the following:

- Systems whose failure to function for even a short period of time could have a severe impact on CMS or the organizations that they support.

- Systems that perform functions with data that are considered to have a high potential for fraud, waste, or abuse.

- Systems that generate, store, process, transfer, or communicate data that are considered to have high sensitivity (Level 3).

8.3.2.4 Level 4: High Criticality and National Security Interest

This category identifies all systems with data processing capabilities that are considered critical to the well-being of CMS. An example would be systems that handle sensitive but unclassified information, the loss of which could adversely affect national security interests.

National Security Directives and other federal government directives require that these systems be protected in proportion to the threat of compromise or exploitation and the associated potential damage to the interest of CMS, its customers, and personnel.

8.4 References

- *Computer Security Act of 1987* (Public Law 100-235). (1988).
- *Privacy Act 1974* (Public Law 93-579, 5 U.S. Code 55a). (1974).
- *Public Information Agency Rules, Opinion Records, and Proceedings (Freedom of Information Act).* (5 U.S. Code 552). (1967).
- *Automated Information Systems Security Program Handbook* (DHHS guide). (October 1995).

CHAPTER 9 - SYSTEM SECURITY PLANS AND CERTIFICATION/ ACCREDITATION

9.1 Overview

The objective of the computer System Security Plan is to ensure the protection of information and information-processing resources. All federal systems have a level of sensitivity and require protection as part of good management practices. This chapter of *The Handbook* provides a description of the CMS System Security Plan (SSP) and Certification/Accreditation process.

9.2 Responsibilities

9.2.1 CMS CIO

The CMS CIO, as the sole accrediting authority, determines the level of acceptable risk for all CMS information resources.

9.2.2 Senior ISSO

The Senior ISSO is responsible to ensure SSP documentation requirements applicable for each accreditation effort are in compliance with federal policies, regulations, and standards.

9.2.3 Senior Systems Security Advisor

The Senior Systems Security Advisor serves as principal advisor and technical authority to the CMS CIO and outside organizations on matters related to systems security.

9.2.4 Component ISSOs (Central and Regional Offices)

Component ISSOs (Central and Regional Offices) have the responsibility to:

- Assist the CMS Senior ISSO in ensuring the component adheres to national systems security policies and procedures.
- Ensure component compliance with CMS's AIS Security Program requirements.
- Act on behalf of the component senior management in the assurance of systems security-related issues.
- Act as the primary point of contact in the component for information security issues.
- Participate in the technical certification of component SSPs.

- Assist component with the development of SSPs during acquisition, development, and systems maintenance.

9.2.5 System Owners/Managers

System Owners/Managers have the responsibility to:

Complete all CMS and Federal requirements for identifying their GSS or MA systems.

Prepare SSPs that provide a description of the security and privacy requirements of the subject system and the plan for meeting those requirements.

Conduct risk assessments, implement controls determined to be required and cost-effective.

Develop contingency and disaster recovery plans that ensure availability of the system for mission accomplishment.

Complete all requirements for system certification. It is the sole responsibility of the System Owner/Manager to ensure that the proper controls have been identified, documented in the SSP and implemented for the system.

Submit the completed SSP Binder to the Security and Standards Group (SSG) for CMS CIO review.

9.3 Policy

All CMS applications and systems must be covered by an SSP(s). The hierarchical structure (see 9.4 System Security Plans) of SSPs applies to any GSS and/or MA to which the system is related. While each system requiring an SSP must develop a separately approved and accredited security plan, the common elements provided in the parent plan are inherited by the subordinate plan by establishing the relationship to a parent GSS or MA and need only reference them. By doing this, a System Owner/Manager is required only to provide information and protections unique to the particular system for which the SSP is being written.

9.4 System Security Plans (SSP)

The purpose of an SSP is to document the operation and security requirements of a system and the controls in place for meeting those requirements. The SSP also delineates responsibilities and the expected behavior of all individuals who access the system.

CMS has implemented the concept of a CMS System Security Master Plan. The Master Plan serves as the enterprise-level security controls that are in place within CMS. The Master Plan will contain all the security attributes that are standard throughout the enterprise such as personnel controls, physical controls for the site, etc. In addition to the Master Plan, CMS has implemented a hierarchical structure for CMS's

System Security Plans. A System Security Plan created by an individual organization inherits the attributes of the plan above and needs only to reference it without repeating the details. For detailed information, see the *CMS System Security Plans (SSP) Methodology.*

9.5 Certification

Certification is based on a technical evaluation of a GSS or MA system to determine how well its security requirements are met. Initial certification must be completed within the component before the system can be forwarded for accreditation review. The ISSO within the component, System Owner/Manager, and System Maintainer must examine the controls implemented for the system and attest to the successful completion of the appropriate technical certification evaluations.

If initial certification is not appropriate, the component ISSO, System Manager/Owner, and System Maintainer can provisionally certify the GSS or MA for operation, with some restrictions and pending specific actions to be completed in a predefined time frame. This interim certification cannot exceed one year. These actions must also be included as milestones in the SSP for the GSS or MA.

GSSs or MAs must be re-certified when substantial changes are made to the GSS or MA, when changes in requirements result in the need to process data of a higher sensitivity, changes occur to authorizing legislation or Federal requirements, and/or changes in the threat environment. Re-certification is also required after the occurrence of a serious security violation which raises questions about the validity of an earlier certification, expiration of conditional accreditation, and at a minimum of every year for GSSs and high risk MAs or every three years for other MAs.

9.6 Accreditation

All CMS GSS and MA systems must receive formal management approval to process through the accreditation process. The CMS CIO or the official management designee reviews the SSP and certification support documentation and either concurs, thereby declaring that a satisfactory level of operational security is present; or does not concur, indicating that the level of risk either has not been adequately defined or reduced to an acceptable level for operational requirements. The CMS CIO or official management designee signs a formal accreditation statement declaring that the GSS or MA appears to be operating at an acceptable level of risk to grant initial approval to process. If initial approval is not granted, the CIO or management designee can either deny accreditation or grant interim accreditation.

An interim accreditation can be granted for a fixed period of time, not to exceed one year. This authority is based on an approved SSP and is contingent on certain conditions being met. This conditional approval to operate, while continuing the management authorization process, permits the GSS or MA to meet its operational mission requirements while improving its computer security posture. If the CMS CIO or the management official designee is not satisfied that the GSS or MA is protected at an

acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. A interim accreditation can be requested by the GSS or MA System Owner/Manager, the System Maintainer, or the CMS component ISSO via an interim certification. An interim accreditation can only be granted by the CMS CIO or the management official designee in lieu of a full denial to process. This conditional approval to operate is not a waiver of the requirement for management approval process. The GSS or MA must meet all requirements and receive management approval to process by the expiration date of the interim accreditation. No extensions of an interim accreditation can be granted except by the CMS CIO or the management official designee.

GSSs and MAs are re-accredited when major changes occur to the GSS or MA (e.g., major changes to system requirements, changes to authorizing legislation or Federal requirements, and/or changes in the threat environment). At a minimum, re-authorization must occur at least every year for GSSs or every three years for MAs, not classified as highly sensitive. Other reasons for re-authorization to process include expiration of an interim certification and/or conditional accreditation.

9.7 References

9.7.1 Laws and Regulations

- *Computer Security Act of 1987* (Public Law 100-235). (1988).

9.7.2 Office of Management and Budget

- *Management of Federal Information Resources* (OMB Circular A-130, Appendix III, Security of Federal AIS). (February 8, 1996).

- *Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information* (OMB Bulletin No. 90-08). July 9, 1990.

- *Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information* (OMB Bulletin No. 88-16). July 1, 1988.

9.7.3 National Institute of Standards and Technology

- *Guide for Developing Security Plans for Information Technology Systems* (NIST Special Publication No. 800-18). (December 1998).

- NIST Security Handbook 800-12: *An Introduction to Computer Security*. (October 1995).

9.7.4 Department of Health and Human Services

- *Automated Information Systems Security Program Handbook* (DHHS guide). (October 1995).

9.7.5 Centers for Medicare & Medicaid Services

- *CMS SSP Methodology. (December 2000)*

CHAPTER 10 - CMS SYSTEM ACCESS

10.1 Overview

System access covers all electronic media by which CMS employees, contractors, and other authorized users of CMS data gain access to CMS systems. On CMS's many multi-user systems, requirements for various computer resources vary considerably. Although it is obvious that users must have access to information they need to do their jobs, it is necessary to deny access to non-job-related information. It is also important to control the kind of access that is afforded (e.g., the ability for the average user to execute, but not change, system programs). These types of access restrictions enforce policy and help ensure that unauthorized actions are not taken. Those working at remote access sites are responsible for following the policies stated herein.

This chapter of *The Handbook* outlines the role and responsibilities for the enforcement of CMS's system access policies. These policies and guidelines apply to CMS employees, contractor personnel and any other authorized users of CMS data.

10.2 Responsibilities

10.2.1 Senior ISSO

The Senior ISSO has the responsibility to:

- Mediate and resolve systems security issues that arise between two CMS organizations, CMS and other federal organizations, or CMS and states or contractors.
- Assist other ISSOs in developing local systems security for either in place System Security Plans or for those under active development.

10.2.2 Component ISSOs (Central and Regional Offices)

Component ISSOs (Central and Regional Offices) have the responsibility to:

- Assist the CMS Senior ISSO in ensuring the component adheres to national systems security policies and procedures.
- Ensure component compliance with CMS's AIS Security Program requirements.
- Develop component systems security guidelines and procedures.
- Assist component RACF Group Administrators with systems security matters.
- Ensure audit trails are used where appropriate, in conjunction with System Owners/ Managers.

10.2.3 System Owners/Managers

System Owners/Managers have the responsibility to:

- Define the system's functionality, configuration, and security requirements.
- Establish the rules for appropriate system use and protection of the subject data and information (rules of behavior) as required by the Privacy Act.
- Implement the SSP and monitor its effectiveness.

10.2.4 System Maintainers/Developers

System Maintainers/Developers are responsible for the development and implementation of security requirements throughout the SDLC at the same time System Owners/Managers define the requirements of the system. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for System Maintainers/Developers), or operational practices (e.g., awareness and training).

10.2.5 Database Administrators

Database Administrators have the responsibility to:

- Certify that systems security requirements of their databases are being met before being moved into a production environment.
- Establish and communicate the security safeguards required for protecting databases based on the sensitivity levels of the data.
- Periodically review and verify that all users of their databases are authorized and are using the required systems security safeguards.

10.2.6 RACF Administrator

CMS's RACF Administrator has the responsibility to:

- Provide leadership and technical guidance in the use of RACF.
- Define the access control strategy for CMS enterprise security management.
- Implement resource access control with RACF for systems' data sets and resources.
- Ensure all CMS components assign RACF Group Administrators for CMS groups and the contractor groups for which they are responsible.

10.2.7 RACF Group Administrators

The RACF Group Administrators have the responsibility to:

- Implementation of RACF within their respective components.
- Control user system access.
- Revoke system access to users when such action is appropriate.
- Define user, group, data set, and connect profiles as required to establish RACF protection for selected group performance.
- Modify component users or data set profiles to control RACF privileges and access to protected resources.
- Enter RACF commands that allow the desired level of user access to protected resources and monitor group performance.
- Assess systems security requirements of group-level data sets.
- Monitor the component's data sets to ensure proper protection of sensitive data.
- Assist users in their assessment of user-identification-level data sets.
- Assist users in determining proper level of protection.
- Reset user passwords when users forget them.

10.2.8 Physical Security Officer

The Physical Security Officers has the responsibility to:

- Ensure physical security of all hardware, software, and information stored and processed in CMS facilities.
- Ensure physical access control services are provided for all facilities.
- Ensure that all facilities fully comply with physical security requirements specified in CMS's AIS Security Program Handbook and DHHS security guidelines.
- Coordinate with management to determine the level of physical security required for facilities based on the sensitivity of the information being processed.
- Specify, implement, and review procedures used to protect the integrity of facilities and operating systems.

- Ensure that the physical security needs of all facilities are identified, incidents are monitored, and corrective actions are taken.

10.2.9 Supervisors

Supervisors at all levels have the responsibility to:

- Authorize employees' appropriate access to job-related resources.
- Provide timely notification of all employee access revocations.
- Ensure that their employees are aware of, and comply with, all of the systems security requirements contained in the CMS AIS Security Program.

10.2.10 Users

Users have responsibility for systems security for the following:

- Ensure the protection of CMS's hardware, software, information, and data by complying with the systems security requirements maintained in CMS AIS Security Program.
- Run application systems and databases only in authorized locations that are certified at a level of systems security equal to or higher than the security level designated for their application systems and databases.
- Ensure that they protect the privacy and confidentiality of all CMS data.
- Ensure confidentiality of their password.

10.3 Access Controls

10.3.1 Resource Access Control Facility (RACF)

RACF is a security management product that allows the CMS enterprise to manage the security features related to the misuse or destruction of computing resources by its users. Through the use of RACF, CMS has the ability to:

- Identify and authenticate users.
- Authorize users to access protected resources.
- Log and report attempts of unauthorized access to protected resources.
- Control the means of access to resources.
- Allow applications to use the RACF macros.

RACF functions by retaining information about the users, resources, and access authorities in profiles are used to determine which users should be permitted access to which protected system resource. CMS's software access control mechanisms are able to identify authorized users trying to gain network access and authenticate the identity of the user. CMS uses a User ID to identify the person who is trying to gain access to the system and a password to authenticate the identity of that user. Therefore, it is important that only the user have knowledge of their password. Each user must keep their password confidential in order to protect system resources.

10.3.2 Mid-Tier Authentication

In addition to RACF, CMS currently uses three additional types of user authentication: NT Domain, Novell NDS and integrated database security.

10.3.3 Remote Access

Policy for remote access controls in compliance with Department directives are currently being negotiated under the MLA between AFGE and the CMS.

10.3.4 CMS Enterprise Password Standard

CMS enterprise systems are comprised of many platforms: NOVELL, OS/390 mainframe, UNIX, NT, ORACLE, and AGNS which, to date, have had their own password rules. To implement password synchronization, and to strengthen the confidentiality of CMS passwords, an enterprise password standard has been developed which will be implemented across all platforms. Our goal is not only to implement password synchronization across platforms, but to ensure that those passwords are complex, hard to crack, and of sufficient length to be secure. The following describes the required minimums for password standards to be enforced on all CMS enterprise systems.

Passwords generated and/or used by CMS users must:

a) be at least six characters in length, but no longer than eight characters;

b) be a mixture of letters and numbers;

c) be changed at least every 60 days;

d) be different from the previous 6 passwords;

e) not contain 4 consecutive characters used from the previous password; and

f) not contain a user's userid;

Systems that authenticate must require passwords of users and must “blacklist” accounts if more than three incorrect attempts are made.

The following factors shall be considered in the design, implementation, and use of a password system used to authenticate the identity of a person or to control access to data. The factors are:

COMPOSITION	The set of acceptable characters which may be used in a valid password.
PATTERN	A set of acceptable password strings
LENGTH RANGE	The set of acceptable lengths of passwords, expressed as a minimum length through a maximum length.
INTERVAL	The maximum acceptable period of time for which a password is valid
HISTORY	The number of acceptable previous passwords to be saved for each userid and compared with a new password.
FAILED ATTEMPTS	Number of consecutive invalid password attempts allowed before the userid is revoked
EXPIRATION WARNING	Number of days before password expiration that the user is to receive a warning message.
CASE SENSITIVE	The password must be upper or lower case.

Passwords must fit the following eight criteria; all CMS systems must enforce these standards to the extent the system is structurally able to enforce them:

Composition *xxxxxxxx*

xxxxxxx

xxxxxx

NOTE: A is alphabetic, x is alpha/numeric and must contain a combination of alpha/numeric or national characters.

Pattern *No 4 consecutive characters of old password.*

Cannot contain userid.

Length Range	*Minimum: 6*
	Maximum: 8
Interval	*60 days*
History	*6*
Failed Attempts	*3*
Expiration warning	*14 days*
Case sensitive	*No*

Users should select passwords that DO NOT contain:

A user's name or nickname

A family member's name

A pet's name

Social Security Number

A birthdate or anniversary

An easily guessed word such as a hobby, favorite sports team or musical group

A variation of a previous password

Such complexity that they must be written down in order to remember them

Users should select passwords that DO contain:

The required mix of letters and numerics

One way to generate acceptable passwords is to use the first letters of an easily recalled saying, such as "Four score and seven years ago", substituting numbers for some words, e.g. f20asya. (Note: Because the password has been used here, f20asya is not a usable password).

10.4 References

10.4.1 Laws and Regulations

- *Computer Security Act of 1987* (Public Law 100-235). (1988).
- *Privacy Act of 1974* (Public Law 93-579, 5 U.S. Code 552a). (1974).

10.4.2 Office of Management and Budget

- *Management of Federal Information Resources* (OMB Circular A-130, Appendix III, Security of Federal AIS). (February 8, 1986).

10.4.3 Department of Health and Human Services

- HHS' Automated Information Systems Security Program Handbook

10.4.4 National Institute of Standards and Technology

- *An Introduction to Computer Security: The NIST Handbook* (NIST Special Publication No. 800-12). (October 1995).

CHAPTER 11 - AUDIT TRAILS

11.1 Overview

With the growth of CMS's dependence on systems resources to support critical agency workloads, and with the availability of those resources to virtually all CMS users at their workstations, CMS-must use audit trails to determine whether those resources are being used for approved purposes. Audit trails are technical controls used by CMS to ensure the integrity of its systems, and to detect, investigate, and support the prosecution of fraud, waste, or abuse.

11.2 Responsibilities

11.2.1 Component ISSOs (Central and Regional Offices)

Component ISSOs (Central and Regional Offices) have the responsibility to:

- Coordinate component reports on suspected systems security violations detected by audit trail process.
- Participate in the technical certification of component SSPs, including documentation of audit trail capabilities.
- Assist component with the development of SSPs during acquisition, development, and systems maintenance, ensuring systems are in compliance with CMS's audit trail policy.
- Ensure audit trails are used where appropriate, in conjunction with System Owners/ Managers.

11.2.2 System Owners/Managers

System Owners/Managers have the responsibility to:

- Define the system's functionality, configuration, and security requirements, including requirements for audit trail capability.
- Ensure a SSP is prepared for each MA and GSS under their authority.
- Officially certify and complete all required certification actions consistent with the CMS SSP Methodology.
- Implement the SSP and monitor its effectiveness.

11.2.3 System Maintainers/Developers

System Maintainers/Developers are responsible for the development and implementation of audit trail security requirements throughout the SDLC.

11.3 Policy

All CMS GSSs and Major Applications must employ audit trail capabilities for the following:

- **Individual Accountability.** The audit trail supports accountability by providing a trace of user actions. Although users cannot be prevented from using resources to which they have legitimate access authorization, audit trail analysis can be used to examine their actions if a suspected security incident is being investigated.

- **Reconstruction of Events.** An organization must use audit trails to support after-the-fact investigations of how, when, and why normal operations ceased.

- **Unauthorized Access.** Audit trails must be designed and implemented to record appropriate information, to assist in determining unauthorized access.

- **Problem Identification.** Audit trails may also be used as on-line tools to help identify problems other than intrusions as they occur. This is often referred to as real-time auditing or monitoring.

11.4 Contents of Audit Trail Records

An audit trail must include sufficient information to establish what events occurred, when they occurred, and who (or what) caused them. Defining the scope and contents of the audit trail must be done carefully as part of the risk assessment to balance systems security needs with possible performance, privacy, or other costs. In general, an event record must specify at a minimum the following:

- **Type of Event.** The type of event and its result, such as failed user authentication attempts, changes to users' systems security information, and organization- and application-specific systems security-relevant events.

- **When the Event Occurred.** The time and day the event occurred must be listed.

- User ID associated with the event.

- Program or command used to initiate the event.

11.5 Audit Trail Security

Organizations must protect the audit trail from unauthorized access. The following precautions must be taken:

- Access to on-line audit logs must be strictly controlled.
- Organizations must strive for separation of duties between security personnel who administer the access control function and those who administer the audit trail.
- The confidentiality of audit trail information also needs to be protected if, for example, it records personal information about users.
- Audit trails must be reviewed periodically based on the level of sensitivity.

11.6 References

- *An Introduction to Computer Security: The NIST Handbook* (NIST Special Publication No. 800-12). (1995).
- *Minimum Security Requirements for Multiuser Operating Systems* (NIST Internal/Interagency Reports [NISTIR] 5153). (March 1993).

CHAPTER 12 - BUSINESS CONTINUITY AND CONTINGENCY PLAN (BCCP)

12.1 Overview

While every effort must be made to avoid disruption of critical applications processed by automated data files and AIS facilities, CMS must also be able to minimize, and be prepared to recover from any disruption that does occur. This chapter of *The Handbook* describes the development, testing, maintenance, and implementation of a BCCP. The information in this chapter applies to all CMS systems and databases, including those provided by contractors, that fulfill mission critical business functions, whether they be a facility, network, major application, or standalone workstation. BCCPs are required as part of the organization's overall AIS Security Program.

12.2 Responsibilities

12.2.1 CMS Management

The CMS Executive Council has the responsibility to designate appropriate systems as critical systems and to rank their criticality.

12.2.2 Senior ISSO

The Senior ISSO is responsible for issuing policy and guidelines for the development of contingency plans as an integral part of the overall CMS AIS Security Program.

12.2.3 System Owners/Managers

System Owners/Managers have the responsibility to:

- Ensure that appropriate contingency plans are developed, periodically tested, and maintained for the systems under their jurisdiction.
- Ensure that the appropriate personnel have been delegated the responsibility for effecting backup operations, and that the backup copies of critical data are maintained, safeguarded, and ready for use in the event of a major disruption.
- Make sure the BCCP is documented, kept up to date, and reviewed periodically.
- Ensure contracts document contingency plan requirements and require contractors to demonstrate the ability to provide continuity of data processing in the event of a disaster.

12.2.4 AIS Facilities Operations Managers

AIS Facilities Operations Managers have the responsibility to:

- Develop and maintain contingency plans, to include designated personnel to be responsible for effecting backup operations in the event of major disruptions.
- Maintain disaster and recovery plans instructions and emergency response procedures.
- Carry out periodic testing of the plan.

12.3 Policy

All CMS GSSs and Major Applications must be covered by a BCCP, identifying the potential consequences of undesirable events and the safeguards needed to counteract their effects. Safeguards included in the BCCP must be selected based on whether they are needed to maintain a minimum level of operation for the affected systems.

Systems Owners/Managers must conduct a risk assessment to gather data to assist in making the above determinations. The results of the risk assessment assist the user by indicating:

- Critical applications and workloads.
- Maximum tolerable delay for the processing of each deferred activity.
- Maximum permissible outage for each application and workload.

12.4 Developing a Business Continuity and Contingency Plan (BCCP)

The following elements must be included in the BCCP for all CMS GSSs and MAs.

12.4.1 Alternate Site

If CMS personnel determine that a lapse in service of a GSS or MA would cause an unacceptable business consequence, then the contingency plan must provide for an alternate site. The alternate site would be used to perform the data processing functions of the organization if a disaster seriously disrupts the services of a principal AIS facility. Furthermore, there must be reasonable assurance that the alternate site be available in the event of a disaster and that it be available for testing the contingency plan.

12.4.2 Hardware

In a disaster recovery situation, compatibility may become the primary concern (e.g., a critical tape must load properly on the backup hardware system). In any approach to contingency planning for a large AIS facility, hardware requirements must be defined to ensure compatibility and sufficient capacity to run critical data until recovery is completed.

12.4.3 Software and Data

CMS personnel must determine the affects of undesirable events on software and data and the correlated affect on CMS services and business operations. Based on this determination and an assessment of risk exposure, CMS personnel must develop a backup cycle for the software and data. The software and data backups must be stored at a secure off-site location. The BCCP must describe the critical software and data, specify how frequently they are backed up, and detail the method of delivery to the off-site secure storage facility location. The plan must also specify how the backup data will be delivered from the off-site secure storage facility to the CMS Off-Site Data Processing Center (ODPC).

12.4.4 Personnel

The BCCP must specifically identify the role of CMS personnel should the plan need to be implemented. The plan must also detail all administrative requirements (i.e., travel authorization, per diem authorization, and lodging). Pre-cleared blanket authorizations may be necessary to move personnel to the CMS ODPC quickly.

12.4.5 Operating Procedures

Operating procedures are specific to the CMS ODPC. They are developed and validated during testing at the CMS ODPC. The plan must identify the critical interfaces that need to be established while recovering from a disaster. For example, continued receipt of electronic updates of Medicare information, especially of a financial nature, is critical to the business of CMS. Continued support of the customer population during the crisis is critical to the maintenance of health and welfare among the customer population.

12.4.6 Recovery

Recovery from a disaster is complete when the principal AIS facility is restored to its original condition, all backlog work is cleared, and the GSSs and MAs are again capable of full operation. The recovery process starts with an assessment of damage to specific equipment, including all the information required in identifying and reordering the equipment.

Accurate inventories and floor plans are invaluable aids in the recovery process. Copies of these items must be a part of the BCCP and must be maintained off-site. To strengthen the plan, it is advisable to work closely with the Contract Office to clear procurement paperwork for hardware and AIS facilities prior to actual need. Once the AIS facility has been physically restored, the final step to return to full operation involves transporting the critical operating software, applications data, and personnel from the CMS ODPC back to the principal AIS facility.

12.4.7 Testing the Plan

The preferred strategy for testing the BCCP is to test each critical application of the AIS facility individually. In this scenario, the software used to run each application is taken to the CMS ODPC to ensure that it runs properly, and to develop and validate its operating procedures. After all critical applications have been run separately, the final test consists of running all of them together at the test site. The results of the final test are then used to complete the plan. After it is completed, the plan must still be tested periodically and updated to accommodate any changes, including any updated versions of the software or critical data.

12.4.8 Implementation

The final step in the BCCP process is determining how to implement the plan in the event of a disaster. This step is vital to overcome any confusion or disorganization that may arise during an emergency. It is especially important for personnel who have specific responsibilities in the recovery operation to practice their roles in a test situation. Implementation procedures must be documented within the plan, and all users must have copies or be thoroughly briefed on pertinent aspects of the plan.

12.5 References

12.5.1 Office of Management and Budget

- *Management of Federal Information Resources* (OMB Circular A-130, Appendix III, Security of Federal AIS). (December 12, 1985).

12.5.2 National Institute of Standards and Technology

- *Guidelines for ADP Contingency Planning* (FIPS Publication 87). (March 1981).

- *Establishing a Computer Security Incident Response Capability* (Special Publication No. 800-3). (November 1991).

12.5.3 Department of Health and Human Services

- *Guidance on Establishing Computer Security Incident Prevention and Response Capabilities* (November 1993).

- *Guide for Protecting Local Area Networks and Wide Area Networks (LANs/WANs).* Draft.

CHAPTER 13 - INTERNET SECURITY

13.1 Overview

The Internet is the fastest growing telecommunications medium in our history. This growth and the easy access it affords has significantly enhanced the opportunity to use advanced information technology for both the public and private sectors. It provides unprecedented opportunities for interaction and data sharing among health care providers, CMS contractors, CMS components, State agencies acting as CMS agents, Medicare and Medicaid beneficiaries, and researchers. However, the advantages provided by the Internet come with a significantly greater element of risk to the confidentiality and integrity of information. The very nature of the Internet communication mechanisms means that security risks cannot be totally eliminated. Up to now, because of these security risks and the need to research security requirements vis-a-vis the Internet, CMS has prohibited the use of the Internet for the transmission of all CMS Privacy Act-protected and other sensitive CMS information by its components and Medicare/Medicaid partners, as well as other entities authorized to use this data.

The Privacy Act of 1974 mandates that federal information systems must protect the confidentiality of individually-identifiable data. Section 5 U.S.C. §552a (e) (10) of the Act is very clear; federal systems must: "...establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." One of CMS's primary responsibilities is to assure the security of the Privacy Act-protected and other sensitive information it collects, produces, and disseminates in the course of conducting its operations. CMS views this responsibility as a covenant with its beneficiaries, personnel, and health care providers. This responsibility is also assumed by CMS's contractors, State agencies acting as CMS agents, other government organizations, as well as any entity that has been authorized access to CMS information resources as a party to a Data Release Agreement with CMS.

However, CMS is also aware that there is a growing demand for use of the Internet for inexpensive transmission of Privacy Act-protected and other sensitive information. CMS has a responsibility to accommodate this desire as long as it can be assured that proper steps are being taken to maintain an acceptable level of security for the information involved.

This issuance is intended to establish the basic security requirements that must be addressed for use of the Internet to transmit CMS Privacy Act-protected and/or other sensitive CMS information.

The term “CMS Privacy Act-protected Data and other sensitive CMS information” is used throughout this document. This phrase refers to data which, if disclosed, could result in harm to the agency or individual persons. Examples include:

- All individually identifiable data held in systems of records. Also included are automated systems of records subject to the Privacy Act, which contain information that meets the qualifications for Exemption 6 of the Freedom of Information Act; i.e., for which unauthorized disclosure would constitute a “clearly unwarranted invasion of personal privacy” likely to lead to specific detrimental consequences for the individual in terms of financial, employment, medical, psychological, or social standing.

- Payment information that is used to authorize or make cash payments to individuals or organizations. These data are usually stored in production application files and systems, and include benefits information, such as that found at the Social Security Administration (SSA), and payroll information. Such information also includes databases that the user has the authority and capability to use and/or alter. As modification of such records could cause an improper payment, these records must be adequately protected.

- Proprietary information that has value in and of itself and which must be protected from unauthorized disclosure.

- Computerized correspondence and documents that are considered highly sensitive and/or critical to an organization and which must be protected from unauthorized alteration and/or premature disclosure.

13.2 Responsibilities

13.2.1 CMS Management

CMS Management has the responsibility to:

- Provide Internet connectivity tools (e.g., equipment, software, and training) to staff within available resources.

- Ensure appropriate use of government equipment and time.

13.2.2 Users

Users have the responsibility to:

- Follow existing security policies and procedures in their use of Internet services and refrain from any practices which might jeopardize CMS computer systems and data files.

- Familiarize themselves with any special requirements for accessing, protecting and utilizing data, including Privacy Act materials, copyrighted materials, and procurement sensitive data.

- Ensure appropriate use of government equipment and time.

13.3 Policy

Note: Use of the Internet is prohibited for health care transactions (claims, remittances, etc.) between Medicare carriers/intermediaries and providers. This Internet prohibition also applies to the transport of CMS Privacy Act-protected data between carriers/intermediaries and any other party. See the CMS Internet Security Policy for a definition of protected data at http://cms.hhs.gov/it/security, and Program Memoranda AB-01-11 (CR 1439) http://cms.hhs.gov/manuals/pm_trans/AB0111.pdf and AB-01-85 (CR 1749) http://www.cms.hhs.gov/manuals/pm_trans/A0185.pdf for this Internet prohibition.

This policy establishes the fundamental rules and systems security requirements for the use of the Internet to transmit CMS Privacy Act-protected and other sensitive CMS information collected, maintained, and disseminated by CMS, its contractors, and agents.

It is permissible to use the Internet for transmission of CMS Privacy Act-protected and/or other sensitive CMS information, as long as an acceptable method of encryption is utilized to provide for confidentiality and integrity of this data, and that authentication or identification procedures are employed to assure that both the sender and recipient of the data are known to each other and are authorized to receive and decrypt such information. Detailed guidance is provided below in item 7. ********

This policy covers all systems or processes which use the Internet, or interface with the Internet, to transmit CMS Privacy Act-protected and/or other sensitive CMS information, including Virtual Private Network (VPN) and tunneling implementations over the Internet. Non-Internet Medicare/Medicaid data communications processes (e.g., use of private or value added networks) are not changed or affected by the Internet Policy.

This policy covers Internet data transmission only. *It does not cover local data-at-rest or local host or network protections. Sensitive data-at-rest must still be protected by all necessary measures, in conformity with the guidelines/rules which govern the entity's possession of the data. Entities must use due diligence in exercising this responsibility.*

Local site networks must also be protected against attack and penetration from the Internet with the use of firewalls and other protections. Such protective measures are outside the scope of this document, but are essential to providing adequate local security for data and the local networks and ADP systems that support it.[1]

13.4 Acceptable Methods

CMS Privacy Act-protected and/or other sensitive CMS information sent over the Internet must be accessed only by authorized parties. Technologies that allow users to prove they are who they say they are (authentication or identification) and the organized scrambling of data (encryption) to avoid inappropriate disclosure or modification must be used to insure that data travels safely over the Internet and is only disclosed to authorized parties. Encryption must be at a sufficient level of security to protect against the cipher being readily broken and the data compromised. The length of the key and the quality of the encryption framework and algorithm must be increased over time as new weaknesses are discovered and processing power increases.

User authentication or identification must be coupled with the encryption and data transmission processes to be certain that confidential data is delivered only to authorized parties. There are a number of effective means for authentication or identification which are sufficiently trustworthy to be used, including both in-band authentication and out-of-band identification methods. Passwords may be sent over the Internet only when encrypted.

13.4.1 ENCRYPTION MODELS AND APPROACHES

Figure 1 depicts three generalized configurations of connectivity to the Internet. The generic model is not intended to be a literal mirror of the actual Internet interface configuration, but is intended to show that the encryption process takes place prior to information being presented to the Internet for transmission, and the decryption process after reception from the Internet. A large organization would be very likely to have the Internet Server/Gateway on their premises while a small organization would likely have only the Internet Client, e.g., a browser, on

---

[1]We note that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) calls for stringent security protection for electronic health information both while *maintained and while in transmission*. The proposed Security Standard called for by HIPAA was published in the Federal Register on August 12, 1998. The public had until October 13, 1998, to comment on the proposed regulation. Based on public comments, a final regulation is planned for late 1999. Policy guidance contained in this bulletin is consistent with the proposed HIPAA security requirements.

premises with the Internet Server at an Internet Service Provider (ISP). The Small User and Large User examples offer a more detailed depiction of the functional relationships involved.

The Encryption/Decryption process depicted graphically represents a number of different approaches. This process could involve encryption of files prior to transmittal, or it could be implemented through hardware or software functionality. The diagram does not intend to dictate how the process is to be accomplished, only that it must take place prior to introduction to the Internet. The ABoundary≅ on the diagrams represents the point at which security control passes from the local user. It lies on the user side of the Internet Server and may be at a local site or at an Internet Service Provider depending upon the configuration.

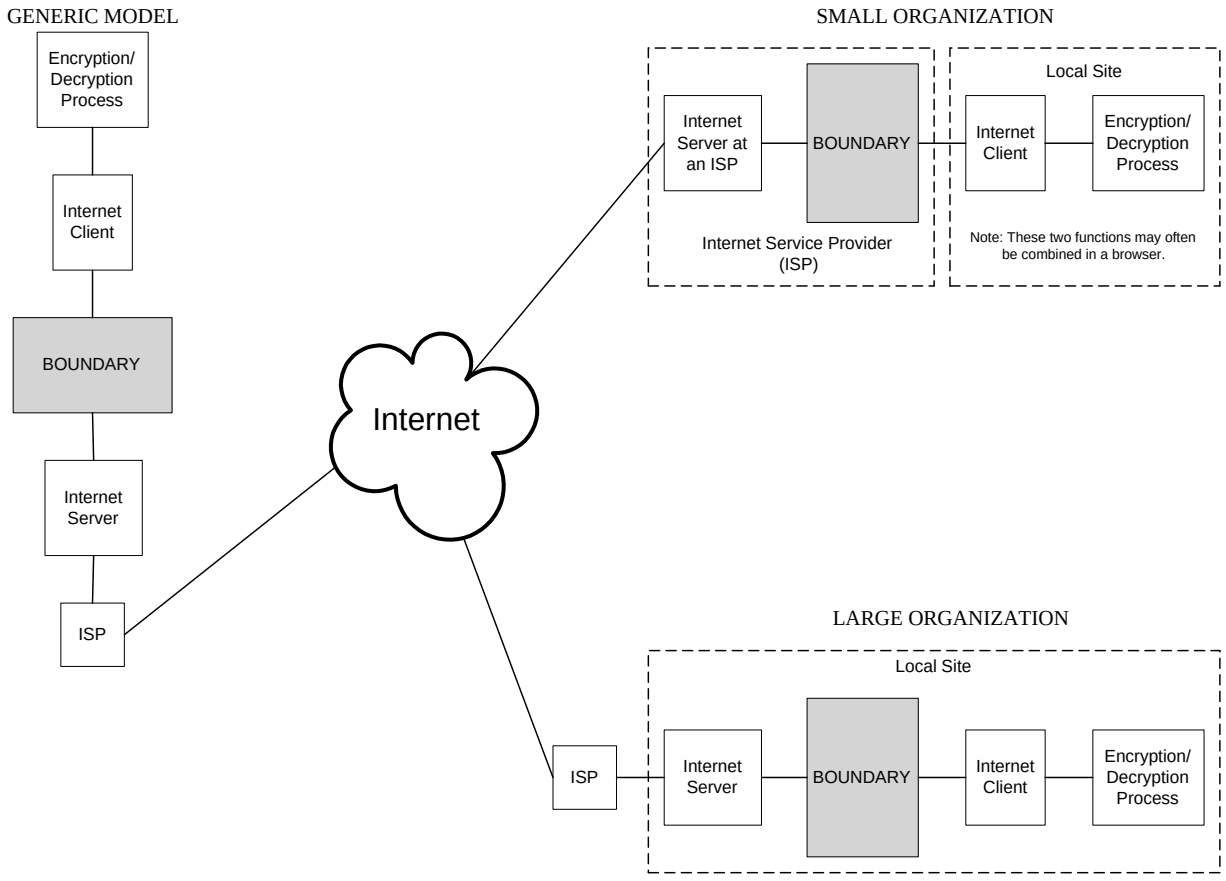


Figure 1: Internet Communications Examples

13.4.2 Acceptable Approaches to Internet Usage

The method(s) employed by all users of CMS Privacy Act-protected and/or other sensitive CMS information must come under one of the approaches to encryption

and at least one of the authentication or identification approaches. The use of multiple authentication or identification approaches is also permissible. These approaches are as generic as possible and as open to specific implementations as possible, to provide maximum user flexibility within the allowable limits of security and manageability.

Note the distinction that is made between the processes of Aauthentication≅ and Aidentification≅. In this Internet Policy, the terms "Authentication" and "Identification" are used in the following sense. They should not be interpreted as terms of art from any other source. Authentication refers to generally automated and formalized methods of establishing the authorized nature of a communications partner over the Internet communications data channel itself, generally called an "in-band process." Identification refers to less formal methods of establishing the authorized nature of a communications partner, which are usually manual, involve human interaction, and do not use the Internet data channel itself, but another "out-of-band" path such as the telephone or US mail.

The listed approaches provide encryption and authentication/identification techniques which are acceptable for use in safeguarding CMS Privacy Act-protected and/or other sensitive CMS information when it is transmitted over the Internet.

In summary, a complete Internet communications implementation must include *adequate encryption*, employment of *authentication or identification* of communications partners, and a management scheme to incorporate *effective password/key management* systems.

13.4.3 Acceptable Encryption Approaches

Note: As of November 1998, a level of encryption protection equivalent to that provided by an algorithm such as Triple 56 bit DES (defined as 112 bit equivalent) for symmetric encryption, 1024 bit algorithms for asymmetric systems, and 160 bits for the emerging Elliptical Curve systems is recognized by CMS as minimally acceptable. CMS reserves the right to increase these minimum levels when deemed necessary by advances in techniques and capabilities associated with the processes used by attackers to break encryption (for example, a brute-force exhaustive search).

HARDWARE-BASED ENCRYPTION:

1. Hardware encryptors - While likely to be reserved for the largest traffic volumes to a very limited number of Internet sites, such symmetric password “private” key devices (such as link encryptors) are acceptable.

SOFTWARE-BASED ENCRYPTION:

2. Secure Sockets Layer (SSL) (Sometimes referred to as Transport Layer Security - TLS) implementations - At a minimum SSL level of Version 3.0, standard commercial implementations of PKI, or some variation thereof, implemented in the Secure Sockets Layer are acceptable.

3. S-MIME - Standard commercial implementations of encryption in the e-mail layer are acceptable.

4. In-stream - Encryption implementations in the transport layer, such as pre-agreed passwords, are acceptable.

5. Offline - Encryption/decryption of files at the user sites before entering the data communications process is acceptable. These encrypted files would then be attached to or enveloped (tunneled) within an unencrypted header and/or transmission.

13.4.4 Acceptable Authentication Approaches

AUTHENTICATION (This function is accomplished over the Internet, and is referred to as an in-band process.)

1. Formal Certificate Authority-based use of digital certificates is acceptable.

2. Locally-managed digital certificates are acceptable, providing all parties to the communication are covered by the certificates.

3. Self-authentication, as in internal control of symmetric “private” keys, is acceptable.

4. Tokens or “smart cards” are acceptable for authentication. In-band tokens involve overall network control of the token database for all parties.

13.4.5 Acceptable Identification Approaches

IDENTIFICATION (The process of identification takes place outside of the Internet connection and is referred to as an “out-of-band” process.)

1. Telephonic identification of users and/or password exchange is acceptable.

2. Exchange of passwords and identities by U.S. Certified Mail is acceptable.

3. Exchange of passwords and identities by bonded messenger is acceptable.

4. Direct personal contact exchange of passwords and identities between users is acceptable.

5. Tokens or “smart cards” are acceptable for identification. Out-of-band tokens involve local control of the token databases with the local authenticated server vouching for specific local users.

13.5 Requirements And Audits

Each organization that uses the Internet to transmit CMS Privacy Act-protected and/or other sensitive CMS information will be expected to meet the stated requirements set forth in this document.

All organizations subject to OMB Circular A-130 are required to have a Security Plan. All such organizations must modify their Security Plan to detail the methodologies and protective measures if they decide to use the Internet for transmittal of CMS Privacy Act-protected and/or other sensitive CMS information, and to adequately test implemented measures.

CMS reserves the right to audit any organization's implementation of, and/or adherence to the requirements, as stated in this policy. This includes the right to require that any organization utilizing the Internet for transmission of CMS Privacy Act-protected and/or other sensitive information submit documentation to demonstrate that they meet these requirements.

13.6 Acknowledgement of Intent

Organizations desiring to use the Internet for transmittal of CMS Privacy Act-protected and/or other sensitive CMS information must notify CMS of this intent. An e-mail address is provided below to be used for this acknowledgment. An acknowledgment must include the following information:

Name of Organization
Address of Organization
Type/Nature of Information being transmitted
Name of Contact (e.g., CIO or accountable official)
Contact's telephone number and e-mail address

For submission of acknowledgment of intent, send an e-mail to: internetsecurity@CMS.gov. Internal CMS elements must proceed through the usual CMS system and project development process.

13.7 Point Of Contact

For questions or comment, write to:

Office of Information Services, CMS
Security and Standards Group
Division of CMS Enterprise Standards -Internet
7500 Security Boulevard
Baltimore, MD 21244

13.8 References

13.8.1 Laws and Regulations

- *Computer Security Act of 1987* (Public Law 100-235). (1988).
- *Privacy Act of 1974* (Public Law 93-579, 5 U.S. Code 552a). (1974).

13.8.2 Office of Management and Budget

- *Management of Federal Information Resources* (OMB Circular A-130, Appendix III, Security of Federal AIS). (February 8, 1996).

CHAPTER 14 - COMPUTER WORKSTATION SECURITY

14.1 Overview

One of the greatest security risks to CMS's assets is at the computer workstation. CMS users are the most important part of minimizing this risk. All users must take actions to safeguard and prevent the improper use of or damage to equipment or data accessible through a workstation.

14.2 Responsibilities

14.2.1 Senior ISSO

The Senior ISSO has the overall responsibility to ensure all users are aware of CMS workstation security policy, procedures and standards.

14.2.2 Component ISSOs (Central and Regional Offices)

Component ISSOs (Central and Regional Offices) have the responsibility to:

- Work with managers to ensure that computer workstation security policies are implemented within their organizations.
- Develop local standard operating procedures specific to the component in compliance with workstation security policy as required.

14.2.3 Supervisors

Supervisors are responsible to ensure their employees comply with computer workstation security policy, guidelines and procedures.

14.2.4 Users

Users are responsible for compliance with computer workstation policy, guidelines and procedures.

14.3 Policy

All CMS workstations must be operated in a manner that ensures:

- Protection of confidentiality of workstation data.
- Display of an appropriate warning banner prior to gaining operating system access.
- Employment of a password protected screen saver and/or NT workstation locking mechanism when the workstation is unattended.

- Proper log off and shut down of workstations at the end of the business day.
- Routine back up of all critical data.
- Virus scanning of media prior to use on any workstation.
- A level of security equivalent to that provided at CMS Central Office for all Alternative Duty Stations.
- Only CMS approved software is used on CMS Central Office and Alternative Duty Station workstations and said software is used in accordance with contract agreements and copyright laws.
- Software copies comply with contract agreements and copyright laws.

14.4 References

14.4.1 Laws and Regulations

- *Federal Managers Financial Act of 1982* (Public Law 97-255, 31 U.S. Code 662). (1982).
- *Privacy Act of 1974* (Public Law 93-579, 5 U.S. Code 552a). (1974).

14.4.2 Office of Management and Budget

- *Management Accountability and Control* (OMB Circular A-123). (February 8, 1996).
- *Financial Management Systems* (OMB Circular No. A-127).
- *Management of Federal Information Resources* (OMB Circular No. A-130).

14.4.3 National Institute of Standards and Technology

- *Security of Personal Computer Systems*: *A Management Guide* (Special Publication No. 500-120). (January 1985).

CHAPTER 15 - SYSTEMS SECURITY INCIDENTS REPORTING AND RESPONSE

15.1 Overview

CMS must protect its computer systems, communication networks, and data from unauthorized use, misuse and abuse by both internal users and external attackers. Confidentiality, integrity, and accessibility of all CMS IT assets must be protected. Protection of CMS assets consists of detecting suspected systems security intrusions, incidents, or violations; reporting all suspected incidents promptly to designated personnel; and taking appropriate steps to investigate them.

Intrusion detection must be accomplished with the use of approved automated detection software tools, both network and host-based. CMS will employ a combination of network and host-based intrusion detection software tools that will provide attack protection and policy enforcement.

15.2 Responsibilities

15.2.1 CMS CIO

The CMS CIO has the responsibility to:

- Ensure an appropriate level of protection for all CMS information resources, whether retained in-house or under the control of contractors, including the establishment of physical, administrative, and technical safeguards.

- Ensure appropriate measures are in place to protect CMS IT assets against unauthorized access that might lead to the alteration, damage, or destruction of information resources, the unauthorized release of data and/or a denial of service, by detecting adverse events in a timely manner.

15.2.2 Senior System Security Advisor

The Senior System Security Advisor has the responsibility to:

- Act as the central point of contact for CMS IT security related incidents or violations.

- Ensure a systems security intrusion reporting system is developed and implemented at CMS.

- Evaluate the severity of any systems security incident.

- Escalate the incident to the CMS CIO and subsequently to the HHS CIO and ISSO, as required, if the incident could potentially have a significant adverse impact on CMS's mission.

15.2.3 Senior Information Systems Security Officer (ISSO)

The Senior ISSO has the responsibility to:

- Initiate an immediate in-house information gathering effort when notified of a suspected security intrusion, incident or security violation.
- Initiate and coordinate the review of all suspected security intrusions, incidents or security violations with the CMS Senior System Security Advisor.

15.2.4 Component ISSOs (Central and Regional Offices)

Component ISSOs (Central and Regional Offices) are responsible to receive the report on suspected security intrusions, incidents or violations and ensure it is reported to the CMS IT Service Desk and the Senior ISSO.

15.2.5 Supervisors

Supervisors have the responsibility to:

- Ensure all suspected security intrusions, incidents or violations are reported to the proper levels.
- Ensure that their employees and contractors know the Security responsibilities and reporting procedures.

15.2.6 All CMS Users

All CMS users who have access to CMS's automated information systems are responsible for reporting actual or suspected security intrusions, incidents or violations to the Action Desk.

15.3 User Reporting Procedures

If you suspect a security incident on any CMS IT asset you use or administer, you must:

- Call the CMS IT Service Desk at 410-786-2580 or 1-800-562-1963 and report the suspected incident.
- Notify the Component ISSO; if you do not know your Component ISSO or cannot locate the person, you must notify the CMS Senior ISSO.
- Notify your immediate supervisor or manager of the suspected security incident.

15.4 References

15.4.1 Laws and Regulations

- Protecting America's Critical Infrastructure: Presidential Decision Directive (PDD) 63. (May 22, 1998).

15.4.2 Office of Management and Budget

- *Management of Federal Information Resources* (OMB Circular A-130, Appendix III, Security of Federal AIS). (December 12, 1985).

15.4.3 National Institute of Standards and Technology

- Guidelines for ADP Contingency Planning (FIPS Publication 87). (March 1981).

- Establishing a Computer Security Incident Response Capability (Special Publication No. 800-3). (November 1991).

15.4.4 Department of Health and Human Services

- Guidance on Establishing Computer Security Incident Prevention and Response Capabilities. (November 1993).

- Guide for Protecting Local Area Networks and Wide Area Networks (LANs/WANs). Draft.

- HHS IRM Policy for Establishing an Incident Response Capability (January 8, 2001).

15.4.5 Public Law

- *Privacy Act of 1974* (Public Law 93-579, 5 U.S. Code 552a). (1974).

CHAPTER 16 - ELECTRONIC MAIL, FACSIMILE, AND OTHER MEDIA SECURITY

16.1 Overview

Because technology is rapidly advancing in the electronic communications area, it is important that CMS protect the privacy, security, and integrity of its communications, as well as ensure the appropriate use of E-Mail, facsimile (FAX) systems, and other kinds of media. This chapter covers all CMS E-Mail, FAX transmissions, including contractor-operated systems that carry or communicate CMS information, and other forms of media. It applies to all employees, contractor personnel, and vendors using CMS systems whose work involves CMS-sponsored software development, software demonstrations, and the operation and maintenance of CMS computer systems.

16.2 Responsibilities

16.2.1 CMS Management

CMS management has the responsibility to:

- Monitor systems security to ensure CMS user compliance with the established policy.
- Authorize, when applicable, the use of E-mail at alternative work sites.
- Ensure that employees are made aware of the CMS E-Mail and FAX policies and ensure that those systems are appropriately used.
- Notify employee in the event their E-Mail or FAX messages are accessed by others.

16.2.2 Senior ISSO

The Senior ISSO has the responsibility to work with management to assure that CMS E-Mail, FAX and Other Media policies are implemented within their organizations.

16.2.3 System Owners/Managers

System Owners/Managers have the responsibility to:

- Formulate and publish CMS E-Mail, FAX, and Other Media policies.
- Maintain efficient and technical operation of the CMS E-Mail system.
- Maintain the integrity and confidentiality of the E-Mail messages.

16.3 Electronic Mail

16.3.1 Background

E-Mail has become an increasingly important method of conducting business within CMS. This increased acceptance has generated questions regarding the security and privacy of the messages and the proper usage of electronic mail systems. E-Mail is not inherently confidential. CMS's E-Mail system contains a built-in feature that encrypts messages when they are stored or sent to an internal CMS recipient. The message does not become readable again until the user retrieves the message. This provides some protection against **unauthorized** reading of E-mail messages.

16.3.2 Policy

The E-mail policy applies to all CMS employees and contractor personnel who use CMS E-Mail. It also applies to all CMS E-Mail being used anywhere on the CMS network, e.g., remote access, WAN, LAN, etc. , and to all contractor-operated systems that carry (or communicate) CMS information. Records and messages which contain classified security information are outside the scope of this policy since CMS does not maintain classified data and the CMS E-Mail system is not rated for classified communications.

CMS provided E-Mail systems are intended for official and authorized purposes only. E-Mail messages are considered by CMS to be government property. Therefore, E-Mail equipment operated by or for CMS staff are subject to the same restrictions on their use as any other government furnished resource provided for use by employees.

Electronic information about an individual in an organized set of records should be protected to the extent that a hard copy record is protected, and disclosed only when required for authorized purposes. Individual specific data of a sensitive nature, whether it be CMS personnel or provider and beneficiary level, must not be transmitted via E-Mail. This includes commercial proprietary information that should be protected in accordance with the conditions under which it is provided.

Information communicated through E-Mail is subject to statutes, regulations, and policies governing the confidentiality and disclosure of Federal government records, including the Privacy Act (PA), the Freedom of Information Act (FOIA), and regulations of the Federal agencies which implement them. This information may be disclosed only for authorized purposes or as otherwise permitted by law.

E-Mail system administrators and others with special system-level access privileges are prohibited from reading electronic messages of others unless authorized by appropriate CMS management officials. However, CMS officials will have access to E-Mail messages whenever there is a legitimate purpose for such access, e.g., technical or administrative problems.

When E-Mail is not in use, users are to exit the software to prevent unauthorized access.

Users are to scan all files to ensure they are virus free before sending or after receiving them through E-Mail.

16.3.3 Password

E-Mail software can only be accessed by using a proper password, created by the user. Users should not share passwords or write the password on a hard copy document where others might read it.

Although users are encouraged to change passwords more frequently, our policy requires users to change passwords every 60 days which is enforced via the E-Mail system.

16.3.4 Privacy/Confidentiality

The contents of Government owned and funded E-Mail are the property of the Government, and, except as required by statute or regulation, CMS cannot guarantee absolute privacy or confidentiality. LAN system administrators and others with special system level access must be authorized by appropriate senior management officials prior to reading the E-Mail of others in the event of technical or administrative problems.

16.3.5 Privacy Act

An E-Mail message or an attachment to the message constitutes a record and provisions of the Privacy Act apply when it is:

a. Retrieved by a person's name, Social Security Number or other personal identifier.

b. Filed, electronically or in hard copy, in a group of similar records for which a notice has been published in the Federal Register informing the public that these records are maintained under the provisions of the Privacy Act.

16.3.6 Freedom Of Information Act

E-Mail messages and attachments are CMS records and are therefore subject to the FOIA. They must be made available upon request, unless one of the nine FOIA exemptions applies. Backup files, including non-record material, remain subject to FOIA requests even if they contain information a user has already destroyed.

(Specific inquiries pertaining to FOIA should be addressed to the CMS Freedom of Information Act Officer, who is solely responsible for making FOIA (E-Mail) disclosure decisions).

16.3.7 Records Management

If an E-Mail record/message would normally be subject to FOIA the sender of that record/message is responsible for making a hardcopy (print) of the record/message and retaining it.

The decision whether a document transmitted via E-Mail is a record that should be filed or deleted is no different than the decision employees make with regard to the disposition of the paper records.

Currently, CMS maintains E-Mail information for 60 days before destroying the information with the exception of information maintained on an individual's PC, which can be maintained indefinitely.

If an E-Mail record/message contains information that should be retained under the Federal Records Management Program, (i.e., Federal Records Act of 1950, as amended (44 U.S.C. Chapters 21,29,31,33); 36 C.F.R., Chapter XII; FIRMR, FPMR), the sender of that record/message is responsible for making a hardcopy (print) of the record/message and retaining it. (Specific inquires pertaining to records management should be addressed to the CMS Records Officer).

16.4 Facsimile

16.4.1 Background

Use of government-provided stand-alone or computer facsimile (FAX) systems is intended only for official and authorized purposes. FAX messages are considered by CMS to be government property. Faxes must be used for Non-Sensitive Data only.

16.4.2 Policy

- Copyright information must be used in accordance with the conditions under which it is provided.

- FAX facilities operated by or for CMS are subject to the same restrictions and review processes as any other government-furnished resource.

16.5 Other Media

16.5.1 Background

Information is CMS's most important asset. Accurate, timely, relevant, and properly protected information is essential to CMS’s business. To ensure that information is properly handled, all accesses to, uses of, and processing of CMS’s information must be consistent with CMS’s information systems related policies and standards. This includes information contained on any magnetic media, compact disk, or paper source.

16.5.2 Policy

16.5.2.1 Data Classification System Labeling Requirements

All tape reels, floppy disks, and other computer storage media containing confidential or privacy information must be externally labeled (marked) with the appropriate sensitivity classification. Paper generated information will also be so labeled.

16.5.2.2 Multiple Copies Only If Reasonable and Customary

Unless permission from the copyright owner(s) is first obtained, making multiple copies of material from magazines, journals, newsletters and other publications is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

16.5.2.3 Release Of Systems Documentation to Third Parties

Prior to being released to third parties, all documentation that describes CMS's systems or systems procedures must be reviewed by the System Owners/Managers to ensure that confidential information is not being inadvertently disclosed.

16.5.2.4 Copying, Transferring, Or Disclosing Software Prohibited

Users must not copy software provided by CMS to any storage media (floppy disk, magnetic tape, etc.), transfer such software to another computer, or disclose such software to outside parties without written permission from the CIO.

16.5.2.5 CMS Data in Hard Copy Form

This section of *The Handbook* provides the security requirements, policies, and procedures for CMS employees, CMS contractors, and others authorized to use CMS data in hard copy form at any site, whether CMS-managed or not; e.g., an individual user's residence, a CMS contractor site, or a hotel room while in travel status.

CMS data in hard copy/display form, whether CMS-managed or not, is display media readable by the human eye, including reports, forms, manuals, memos, letters, wires, microform (microfiche and microfilm), used carbon paper, used typewriter ribbons, and printer ribbons. The acceptable methods of protecting CMS data in hard copy form are as follows (See Chapter 8 - for Security Level Designations)

Level 1: Low Sensitivity:

- Retain a backup photocopy at the standard workplace.
- Protect from water, heat and other damage.
- If disposing of the hard copy document, no special security efforts are necessary.

Level 2: Moderate Sensitivity:

- Retain a backup photocopy at the standard workplace.
- Protect from water, heat and other damage.
- Keep the hard copy document from view of unauthorized persons at all times.
    - In transit, do so via a securable container such as a briefcase.
    - During use, keep others away.
    - When not in use, physically secure the hard copy document, as in a locked drawer or container for which no unauthorized person(s) has a key. Also, secure the room where the hard copy document is kept.
- If disposing of the hard copy document, finely shred it (fragments less than 3/32" in at least one dimension).

Level 3: High Sensitivity:

- Retain a backup photocopy at the standard workplace.
- Protect from water, heat and other damage.
- Taking highly sensitive information outside the standard workplace requires explicit management approval.
- Keep the hard copy document from view of unauthorized persons at all times.
    - In transit, do so via a securable container such as a briefcase.
    - During use, keep others away.
    - When not in use, physically secure the hard copy document, as in a locked drawer or container for which no unauthorized person(s) has a key. Also, secure the room where the hard copy document is kept.
- If disposing of the hard copy document, finely shred it (fragments less than 3/32" in at least one dimension).
- Owners (and/or providers of the data to the user) may require limited distribution handling which could involve:
    - Assigning numbers to individual copies;
    - Retaining a list of persons who received copies; and

- Explicit disposal methods.

16.6 References

- *Freedom of Information Act* (Public Law 90-23, 5 U.S. Code 552). (1967).
- *Freedom of Information Act* (Public Law 93-502, Amendments). (1974).
- *Privacy Act of 1974* (Public Law 93-579, 5 U.S. Code 552a). (1974).

CHAPTER 17 - ACQUISITIONS AND CONTRACTS

17.1 Overview

All contractors who are involved in developing GSSs and MAs for use by CMS, or in providing any other type of service for CMS in which Federal IT resources are used, must agree to comply with the requirements of the CMS AIS Security Program.

This chapter of *The Handbook* describes the CMS AIS Security Program policy for establishing the systems security requirements for solicitations and contracts. All contractors must adhere to the policy guidelines presented in this chapter.

17.2 Exclusion of Grants and Cooperative Agreements

Grants and cooperative agreements are excluded from the policy described in this chapter of *The Handbook*. However, when appropriate, grantees and participants in cooperative agreements are encouraged to implement adequate AIS security safeguards. CFR 45, Part 74 establishes uniform administrative requirements for recipients of federal funds to provide effective control and accountability for all government-furnished assets.

17.3 Responsibilities

17.3.1 Project Officer

Whenever a contract involves the development of a GSS or MA or the use of AIS resources, the awarding organization must designate a Project Officer to oversee the technical requirements of the proposed contract effort, to participate in the evaluation of the technical proposal(s), and to monitor the performance of the contractor. The Project Officer has the responsibility to:

- Conduct a preliminary security-sensitivity assessment as part of the needs determination and conduct an analysis of systems security requirements as part of the requirements analysis (or ensure that these analyses are conducted) and including copies of the analyses in the program office official files.

- Specify the systems security requirements for inclusion in the SOW.

- Certify that the SOW complies with the requirements of the CMS AIS Security Program and obtain the signature of the Component ISSO on the certification statement.

- Develop an evaluation plan to be used to assess whether the proposal meets the minimum-systems security requirements and whether the offeror can comply with the systems security provisions of the prospective contract.

- Conduct a technical review, in accordance with the evaluation plan, of proposals received in response to the RFP and determine which proposals meet the systems security requirements specified in the SOW and which demonstrate the ability to comply with the systems security provisions of the prospective contract.

- Certify that successful proposals comply with the requirements of the CMS AIS Security Program and obtain the signature of the Component ISSO on the certification statements.

- Conduct an on-site inspection and test of the offeror's computer information security safeguards if specified in the SOW and the evaluation plan.

- Monitor, on an ongoing basis, contractor adherence to systems security provisions.

17.3.2 System Owners/Managers

System Owners/Managers have the responsibility to:

- Work with the Project Officer, Contracting Officers, and Component ISSOs to ensure that RFPs pertain to their application systems, GSSs, and MAs comply with the CMS AIS Security Program.

- Participate, as appropriate, in the technical review of proposals received in response to RFPs.

17.3.3 Senior ISSO

The Senior ISSO is responsible to provide assistance to Project Officers and to System Owners/Managers in carrying out their roles and responsibilities.

17.3.4 Component ISSOs

The Component ISSOs have the responsibility to:

- Provide assistance to Project Officers and to System Owners/Managers in carrying out their roles and responsibilities.

- Review and sign Agency Procurement Requests as well as the Solicitation Certifications and Pre-Award Certifications. For example, the Component ISSOs confirm, by signing the Pre-Award Certification, that the successful proposals received in response to an RFP and certified by the Project Officer comply with the requirements of the CMS AIS Security Program. This responsibility to review and sign Agency Procurement Requests as well as the Solicitation Certifications and Pre-Award Certifications are delegated as appropriate by the CMS CIO.

17.3.5 Contracting Officers

Contracting Officers are responsible for taking the following actions on procurements that involve the development of GSSs or MAs or the use of AIS resources:

- Ensure that the Pre-Award Certification statements of AIS security requirements for successful proposals are signed by both the Project Officer and the Component ISSO and are submitted with the proposals. The Contracting Officer initiates action on a proposal when a properly executed certification statement is received.

- Include a statement in the RFP requiring offerors to present a detailed outline of their proposed AIS security program in their proposals.

- Include a statement in the RFP that offerors are required to comply with the SOW and with the requirements of the CMS AIS Security Program. The statement must read substantially as follows:

  > *The Contractor agrees to comply with the AIS security requirements set forth in the Statement of Work and applicable portions of the CMS Information Systems Security Policy, Standards and Guidelines Handbook. The contractor further agrees to include this provision in any subcontract awarded pursuant to the prime contract.*

- Include a statement in the RFP requiring winning contractors to pay the costs of required security background investigations.

- Furnish copies of *The Handbook* when requested by offerors who respond to the RFP.

- Forward to the Component ISSOs any forms that the winning contractor must submit to verify or obtain personnel security background investigations for the contractor's staff. If the winning contractor's personnel have not undergone required background investigations, the awarding organization is responsible for assisting the contractor in obtaining the investigations. When it is necessary to begin contract work without the appropriate investigations, contractor personnel may begin parts of the work that are not sensitive. They must be closely monitored until investigations have been completed; if approval cannot be obtained, contractor personnel must be replaced. If a waiver is necessary, contact the Agency PSR.

- Ensure that the technical evaluation reports on successful proposals developed by the Project Officer either detail any AIS security deficiencies or confirms contractor compliance with requirements.

17.4 Policy

In accordance with the requirements of the CMS AIS Security Program, every Request for Proposal (RFP) that involves the development of a GSS or an MA, or the use of AIS

resources, must include appropriate systems security requirements. Systems security requirements must be considered in all phases of the procurement cycle: planning, solicitation, source selection, and award and contract administration. Contractors who perform direct AIS services, including time-sharing service contractors, must meet these requirements. The requirements also apply to contractors who participate in the design, development, operation, or maintenance of AIS telecommunications systems for CMS. All contractors are required to safeguard the application systems, software packages, personal data, sensitive data, trade secrets, and other CMS AIS assets against destruction, loss, or misuse.

17.5 Planning for an Acquisition or Contract

OMB Circular A-130, Appendix III, requires that agencies define and approve security requirements and specifications before acquiring or starting formal development of applications, specifically to:

- Identify systems security and privacy requirements in the requirements analysis.

- Identify systems security requirements necessary to protect classified and sensitive information by listing the potential threats and hazards, and describing the measures needed to provide protection.

- Identify physical and environmental security safeguards.

The systems security requirements must be determined using *The Handbook* and must be based on the technical requirements of the contract. The systems security requirements must substantiate an overall security level designation that is commensurate with the value, sensitivity, or criticality of the resources or services to be provided by a contractor.

Useful guidance for incorporating computer systems security into the resources procurement cycle, starting with initial planning for the acquisition, is presented in NIST Special Publication 800-4, Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials. Key elements of this guidance to be addressed during the acquisition planning stage include the following:

- Conduct a preliminary sensitivity assessment as part of the determination of needs. The preliminary sensitivity assessment defines the basic computer systems security needs of the planned system, expressed in terms of integrity, availability, and confidentiality. The preliminary sensitivity assessment is a high-level analysis that provides a framework for further analysis.

- Conduct an analysis of systems security needs as part of the requirements analysis, including:

- A specific analysis of integrity, availability, and confidentiality, including an analysis of applicable laws and regulations as well as functional and other systems security requirements. If necessary, the preliminary sensitivity assessment should be updated based on the results of the requirements analysis.

- An analysis of the level of assurance required, or the degree to which it is known that the security features and procedures being acquired will operate correctly, and will prove to be effective, in the intended operating environment.

- A planning phase risk assessment, as required by OMB Circular A-130, Appendix III. The planning phase risk assessment incorporates input from the analysis of integrity, availability, and confidentiality; the analysis of the level of assurance required; and the sensitivity assessment. A determination of what types of controls will be cost-effective is made as part of the planning phase risk assessment.

17.6 Solicitation of FIP Resources

17.6.1 Statement of Work

OMB Circular A-130, Appendix III, states the following:

- The SOW must include appropriate AIS security requirements. The AIS security requirements must be sufficiently detailed to enable offerors to understand what is required. A general statement that the offeror must agree to comply with applicable requirements is not acceptable. The systems security requirements must be determined by using *The Handbook* and should be based on the requirements analysis, as appropriate:

  - Agency rules of conduct that a contractor shall be required to follow.

  - A list of the anticipated threats and hazards that the contractor must guard against.

  - A description of the safeguards that the contractor must specifically provide.

  - The systems security standards applicable to the contract.

  - A description of the test methods, procedures, criteria, and inspection system necessary to verify and monitor the operation of the safeguards during contract performance and to discover and counter any new threats or hazards.

  - A description of the procedures for periodically assessing the systems security risks involved.

  - A description of the personnel security requirements.

- Consistent with the guidelines for Federal computer systems security training issued by NIST and regulations issued by the OPM, a description of the systems security training that the contractor is required to provide to its employees.

- Consistent with the guidelines issued by the OMB in the OMB Bulletins on systems security, a description of the plan the contractor must develop or follow to provide for the security and privacy of resources the contractor is required to operate.

- In addition to appropriate specifications, specific items to be included in the SOW are:

  - An explicit statement of the security level designation.

  - A list of the minimum-systems security and safeguard requirements commensurate with the security level designation.

- The SOW also must include special provisions to address contractor employees associated with the project for the following:

  - "Persons without required background investigations cannot perform any critical/sensitive contract work until their investigations are completed or initiated."

  - "Persons without necessary background investigations will not have access to sensitive project data."

  - "Persons without necessary security clearances will not have access to classified national security information."

  - "All contractor personnel designated as Levels 5C and 6C, or others as deemed necessary, who are directly performing the work of the contract, particularly those who work in CMS facilities or who have access to CMS equipment or sensitive data, must be named in the contract and must be subject to a key personnel clause."

  - "Violation of any of these conditions may lead to termination of the contract."

- A request that offerors include a copy of their standard security policy and practices in their proposals must address the following:

  - A description of the facilities they will be using during the project and the security features of these facilities.

  - The procedures for handling or accessing Government data and other AIS resources during the performance of the contract.

  - The physical storage procedures to be used to protect Government data and other resources during performance of the contract.
  - Any required limitations on employees concerning the reproduction, transmission, or disclosure of data and project information.
  - Any required time-sharing procedures employees must follow during performance of the contract, if applicable.

- Procedures for the destruction of source documents, storage media, and other related waste material.
- A request that the offeror acknowledge understanding of the systems security requirements detailed in the SOW.
- A request that the offeror acknowledge understanding of the requirement that the Project Officer approve the use by the contractor of any subcontractors, vendors, or suppliers prior to their use.
- A request that the offeror provide a copy of the offeror's organizational chart which shows the proposed personnel descriptions, so the Project Official can determine position sensitivity designations.
- A request that the offeror provide a brief description of the responsibilities of each position on the offeror's organizational chart, so that the personnel security designations can be evaluated.

17.6.2 AIS Security Standards

Applicable CMS standards plus federally mandated AIS security standards must be included in the SOW. The following publications contain lists of federally mandated AIS security and other standards:

- NIST Publication List 58, *FIPS Publications Index*.
- NIST Publication List 88, *Computer Systems Publications*.
- NIST Publications List 91, *Computer Security Publications*.
- GSA Handbook, *Federal ADP and Telecommunications Standards Index*.
- NISTIR 4749, *Sample SOW for Federal Computer Security Services: For Use In-House or Contracting Out*, provides useful examples of wording that may be incorporated into SOWs for computer security activities.

17.7 Evaluation Plan

The evaluation plan will be used to determine whether the offeror's assurances of AIS security-related claims are true and whether the offeror can provide the proposed services. The evaluation plan must be developed in concert with the SOW. It will be used to help develop sections of the SOW that give the offeror instructions for providing assurance of AIS security. If an on-site inspection or testing of computer systems security assurances is to be part of the evaluation, then the inspection or testing required must be specified in the SOW. NIST Special Publication Number 800-4, Appendix B, "Assurance," provides guidance on preparing an evaluation plan.

17.7.1 Source Selection and Award

The procedure for evaluating proposals received in response to the RFP and for awarding the contract for services is as follows:

- The Contracting Officer forwards the computer systems security components of each proposal to the Project Officer or the Component ISSO for review and evaluation, and the Project Officer and the Component ISSO determine that all of the systems security requirements listed in the SOW for the contract are addressed in the proposal.

- The Project Officer, following the evaluation plan, conducts a technical review of the proposal with other evaluation team members to determine the adequacy and capability of the contractor to meet the systems security requirements listed in the SOW for the contract.

- The Project Officer develops a technical evaluation report on the proposal.

- The Project Officer and the Component ISSO certify that the proposal complies with the systems security requirements specified in the SOW and the requirements of the CMS AIS Security Program; they then attach the technical evaluation report to the certification.

- If required in the evaluation plan and specified in the SOW, the Project Officer or the Component ISSO conduct an on-site inspection of the offeror's facilities to ensure that facility safeguards are commensurate with the sensitivity of data and the value of the assets to be protected during performance of the contract. The Project Officer provides written confirmation of findings from the inspection to the Contracting Officer.

- If required in the evaluation plan and specified in the SOW, the Project Officer or the Component ISSO conduct testing of the offeror's computer systems security assurances to ensure that the required level of assurance is commensurate with the sensitivity of data and the value of the assets to be protected during performance of the contract. The Project Officer provides written confirmation to the Contracting Officer that required information security safeguards meet the testing criteria.

When the Contracting Officer has received written confirmation that the required information security safeguards are in place and that any required testing was satisfactory, the contracting officer may award the contract. The Contracting Officer must include a policy statement similar to the "Security Policy Statement for Inclusion in Automated Information Systems Contracts," in the contract.

17.7.2 Contract Administration

After the contract has been awarded, the Project Officer, Component ISSO, and System Owners/Managers, in coordination with the assigned Contracting Officer, must conduct periodic reviews of the project to ensure that security is maintained at the appropriate level and that there is continued compliance with the CMS AIS Security Program. All instances of noncompliance must be reported to the Contracting Officer, or designated representative, for necessary action.

17.7.3 Incumbent Contracts

Contracting Officers and Project Officers must negotiate reasonable time frames for incumbent contractors to comply with the policy presented in this chapter. As a first step, incumbent contractors must be required to comply with applicable personnel security requirements. All personnel who directly perform contract work that requires completion of a favorable background investigation must obtain appropriate security certification.

17.8 References

17.8.1 Laws and Regulations

- *45 Code of Federal Regulations, Part 74.*

17.8.2 Office of Management and Budget

- *Management of Federal Information Resources* (OMB Circular A-130, Appendix III, Security of Federal AIS). (December 12, 1985).

17.8.3 General Services Administration

- *Requirements Analysis* (FIRMR Subpart 201-20.1).
- *Security and Privacy* (FIRMR Subpart 201-21.3).
- *Security Specifications* (FIRMR Subpart 201-39.1001-1).
- *Federal ADP and Telecommunications Standards Index*.

17.8.4 National Institute of Standards and Technology

- (NIST Publication List 58) Federal Information-Processing Standards (FIPS PUBS) Index.
- NIST Publication List 88, *Computer Systems Publications*.
- NIST Publications List 91, *Computer Security Publications*.
- NISTIR 4749, *Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out*, December 1991.
- *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials* (Special Publication No. 800-4). (March 1992).

APPENDIX A - ACRONYMS AND ABBREVIATIONS

ACRONYM/ ABBREVIATION	DEFINITION
A	
ACL	Access Control Lists
ADP	Automated Data Processing
AIS	Automated Information Systems
AIS-STOP	Automated Information Systems Security Training and Orientation Program
B	
BCCP	Business Continuity and Contingency Plan
C	
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIRC	Computer Incident Response Capability
CMS	Centers for Medicare & Medicaid Services
D	
DES	Data Encryption Standard
DHHS	Department of Health and Human Services
DLTS	Division of Legal and Technical Services
DHR	Director of Human Resources
DOS	Denial Of Service
E	
E-Mail	Electronic Mail
F	
FAX	Facsimile

ACRONYM/ ABBREVIATION	DEFINITION
FIPS	Federal Information Processing Standards
FOIA	Freedom of Information Act
G	
GSA	General Services Administration
GSS	General Support Systems
I	
IP	Internet Protocol
IPMG	Investment Planning and Management Group
IRM	Information Resources Management
ISSO	Information Systems Security Officer
IT	Information Technology
ITIRB	IT Investment Review Board
L	
LAN	Local Area Network
LBI	Limited Background Investigation
M	
MA	Major Application
N	
NAC	National Agency Check
NACI	National Agency Check and Inquiries
NACIC	National Agency Check and Inquiries and Credit
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal/Interagency Reports

ACRONYM/ ABBREVIATION	DEFINITION
O	
ODPC	Off-Site Data Processing Center
OGC	Office of General Counsel
OGE	Office of Government Ethics
OIRM	Office of Information Resources Management
OIS	Office of Information Services
OMB	Office of Management and Budget
OPM	Office of Personnel Management
P	
PC	Personal Computer
PIN	Personal Identification Number
PSO	Physical Security Officer
PSR	Personnel Security Representative
R	
RACF	Resource Access Control Facility
RFP	Request for Proposal
S	
SAC	Special Agreement Checks
SDLC	System Development Life Cycle
SF	Standard Form
SOR	System of Records
SOW	Statement of Work
SPO	Servicing Personnel Officer
SSATE	Systems Security Awareness Training and Education
SSBI	Single Scope Background Investigation
SSP	System Security Plan

ACRONYM/ ABBREVIATION	DEFINITION
U	
User ID	User Identification
W	
WAN	Wide Area Network
WWW	World-Wide Web

APPENDIX B - GLOSSARY

TERM	DEFINITION
ACCESS TO INFORMATION	The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.
ACCREDITATION	The official management (i.e., CMS CIO) authorization for the operation on an application and is based on the certification process as well as other management considerations. (FIPS Publication 102)
AGENCY	Any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only the Office of Management and Budget and Office of Administration. (OMB Circular A-130)
AGENCY-OWNED OR LEASED EQUIPMENT OR RESOURCES	"Agency-owned or leased equipment and resources includes, but is not limited to, computer systems (including Internet and E-mail), photocopiers, facsimile machines, telephones or audio-visual equipment." (2004 Master Labor Agreement)
APPLICATION SYSTEM	Computer system written by or for a user that applies to the user's work; for example, a payroll system, inventory control system, or a statistical analysis system. (FIPS Publication 11-3)
ASSETS	These include information, software, personnel, hardware, and physical resources (such as the computer facility).
ASSET VALUATION	The value of an asset consists of its intrinsic value and the near-term impacts and long-term consequences of its compromise.
AUTOMATED INFORMATION SYSTEM (AIS)	The organized collection, processing, transmission, and dissemination of automated information in accordance with defined procedures. (OMB Circular A-130)
AIS ASSET	Any software, data, hardware, administrative, physical, communications, or personnel resource within an ADP system or activity. (NISTIR 4659)

TERM	DEFINITION
AIS FACILITY	An organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. [AIS facilities range from large centralized computer centers to individual standalone workstations.] (OMB Circular A-130)
AIS SECURITY (COMPUTER SECURITY)	The concepts, techniques, technical measures, and administrative measures used to protect the hardware, software, and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification, use, or loss. (FIPS Publication 11-3)
AVAILABILITY	Assurance that there exists timely, reliable access to data by authorized entities, commensurate with mission requirements.
CERTIFICATION	A technical evaluation with system owner's concurrence of a sensitive application and/or system to see how well it meets security requirements. (FIPS Publication 102)
COMPUTER SYSTEM	Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources as defined by regulations issued by the Administrator for General Services pursuant to E-Mail 111 of the Federal Property and Administrative Services Act of 1949. (Computer Security Act of 1987) "Computer systems are any assembly of computer hardware, software, peripherals or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data." (2004 Master Labor Agreement)
CONFIDENTIALITY	Assurance that data is protected against unauthorized disclosure to individuals, entities or processes.

TERM	DEFINITION
CONSEQUENCE ASSESSMENT	An estimation of the degree of overall, aggregate harm or loss that could occur, e.g., lost business, failure to perform the system's mission, loss of reputation, violation of privacy, injury, or loss of life.
CONTINGENCY PLAN	A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan. (FIPS Publication 11-3)
CONTINGENCY PLANNING	A planned response to high impact events to maintain a minimum acceptable level of operation.
DATABASE	A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; data is stored so that it can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data. (FIPS Publication 11-3)
DATABASE MANAGER	The official who is responsible for the operation and use of a database. (DHHS Definition)
DATA ENCRYPTION SYSTEM (DES)	A commonly used secret-key cryptographic algorithm for encrypting and decrypting data, developed by the National Institute of Standards and Technology (NIST) as a Federal Information Processing Standard (FIPS). (FISCAM) DES was adopted by the U.S. Government as FIPS Publication 46 [at Publication 46-1], which allows only hardware implementations of the data encryption algorithm. (FIPS Publication 11-3).
DISASTER RECOVERY	A plan for the restoration of lost data, or the reconciliation of conflicting or erroneous data, after a system failure due to natural or manmade disaster.
DISSEMINATION OF INFORMATION	The function of distributing Government information to the public, whether through printed documents, or electronic or other media. Dissemination of information does not include intra-agency use of information, interagency sharing of information, or responding to public requests for access to information. (OMB Circular A-130)

TERM	DEFINITION
ENCRYPTION	The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission, or when it is stored on a transportable magnetic medium. (Microsoft Press Computer Dictionary)
FEDERAL COMPUTER SYSTEM	A computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function. A Federal computer system includes automatic data processing equipment as that term is defined in E-Mail 111(a)(2) of the Federal Property and Administrative Services Act of 1949. (Computer Security Act of 1987)
FIREWALLS	Hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users. (FISCAM)
GENERAL SUPPORT SYSTEMS (GSS)	An interconnected set of information resources under the same direct management control which shares common functionality. -A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network. A departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. (OMB Circular A-130)
GUIDELINES	General statements that are designed to achieve the policy's objectives by providing a framework within which to implement procedures.
HACKER	A person who secretively invades others' computers, inspecting or tampering with the programs or data stored on them. (Microsoft Press Computer Dictionary)

TERM	DEFINITION
ILLEGAL ACCESS AND DISCLOSURE	Activities of employees that involve improper systems access and sometimes disclosure of information found thereon, but not serious enough to warrant criminal prosecution. These cases should be entered on the Fraud Monitoring and Reporting System.
INFORMATION	Any communication or reception of knowledge, such as facts, data, or opinions; including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape. (OMB Circular A-130)
INFORMATION RESOURCES MANAGEMENT (IRM)	The planning, budgeting, organizing, directing, training, and control associated with Government information. The term encompasses both the information itself and related resources, such as personnel, equipment, funds, and technology. (OMB Circular A-130)
INFORMATION SYSTEMS SECURITY (INFOSEC)	The protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and information contained in the systems. [Protection results from the application of a combination of security measures, including cryptosecurity, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.] (NISTIR 4659)
INTEGRITY	Assurance that data is protected against unauthorized, unanticipated, or unintentional modification and/or destruction.
INTERNET	A worldwide electronic system of computer networks which provides communications and resource sharing services to government employees, businesses, researchers, scholars, librarians and students as well as the general public.
LIMITED BACKGROUND INVESTIGATION (LBI)	The NACI, credit search, personal subject interview, and personal interviews by an investigator of subject's background during the most recent three years. (ISSPH – Glossary)

TERM	DEFINITION
LOCAL AREA NETWORK (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network. (Microsoft Press Computer Dictionary) Local area networks commonly include microcomputers and shared (often-expensive) resources such as laser printers and large hard disks. Most modem LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks. (FISCAM)
MAJOR APPLICATION (MA)	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, modification of, or unauthorized access to the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the system in which they operate. (OMB Circular A-130)
MALICIOUS SOFTWARE	The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms. (DHHS Definition, adapted from NIST Special Publication 500-166)
MEDIA	Hard copy (including paper), PC/ workstation diskettes, and other electronic forms by which CMS data is stored, transported, and exchanged. The need to protection information confidentiality, integrity, and availability applies regardless of the medium used to store the information. However, the risk exposure is considerably greater when the data is in an electronically readable or transmittable form compared to when the same data is in paper or other hard copy form.
MISUSE OF GOVERNMENT PROPERTY	The use of computer systems for other than official business that does not involve a criminal violation, but is not permissible under CMS policies.

TERM	DEFINITION
MODEM	Modem is short for modulator/demodulator, a communications device that enables a computer to transmit information over a standard telephone line. Modems convert digital computer signals into analog telephone signals (modulate) and the reverse (demodulate). (Microsoft Press Computer Dictionary)
NATIONAL AGENCY CHECK (NAC)	An integral part of all background investigations, the NAC consists of searches of OPM's Security/Suitability Investigations Index (SII); the Defense Clearance and Investigations Index (DCII); the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary. (ISSPH – Glossary)
NAC and INQUIRIES (NACI)	The basic and minimum investigation required on all new Federal employees. It consists of a NAC with written inquiries and searches of records covering specific areas of a person's background during the past five years. Those inquiries are sent to current and past employers, schools attended, references, and local law enforcement authorities. (ISSPH – Glossary)
NACI and CREDIT (NACIC)	This NACI includes the addition of a credit record search and is the minimum investigation for those going into low risk public trust positions (Level 1).
NETWORK	A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables or temporary connections made through telephone or other communications links. A network can be as small as a LAN consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area. Small or large, a computer network exists to provide computer users with the means of communicating and transferring information electronically. (Microsoft Press Computer Dictionary)

TERM	DEFINITION
PASSWORDS	A confidential character string used to authenticate an identity or prevent unauthorized access. (FISCAM) Passwords are most often associated with user authentication. However, they are also used to protect data and applications on many systems, including PCs. Password-based access controls for PC applications are often easy to circumvent if the user has access to the operating system (and knowledge of what to do).
PERSONNEL SECURITY	Personnel security refers to the procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is commensurate with the value of ADP resources which the individual will be able to access. (NISTIR 4659)
PHYSICAL CRIMES	Physical crimes against CMS employees or property. This category includes information brokering and other access and disclosure incidents of a serious nature so as to constitute a criminal violation. Physical crimes are also actions taken by CMS employees, beneficiaries, or third parties to defraud the Administration, usually for monetary gain. These cases should be referred to the Office of the Inspector General and entered on the Fraud Monitoring and Reporting System.
PHYSICAL SECURITY	The application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information. (NISTIR 4659)
POLICY	A high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area.
PROCEDURES	Define the specifics of how the policy and the supporting standards and guidelines will actually be implemented in an operating environment.

TERM	DEFINITION
RISK	The potential for harm or loss. Risk is best expressed as the answers to these four questions: 1. What could happen? (What is the threat?) 2. How bad could it be? (What is the impact or consequence?) 3. How often might it happen? (What is the frequency?) 4. How certain are the answers to the first three questions? (What is the degree of confidence?) The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no "risk" per se. (HISM)
RISK ASSESSMENT	The identification and study of the vulnerability of a system and the possible threats to its security. (FIPS Publication 11-3)
RISK MANAGEMENT	The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. (NISTIR 4659)
SAFEGUARD ANALYSIS	An examination of the effectiveness of the existing security measures, actions, devices, procedures, techniques, or other measures that reduce a system's vulnerability to a threat and identification of appropriate new security measures that could be implemented on the system.

TERM	DEFINITION
SECURITY	All of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from without and from misuse from within. Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting privacy of the individuals who are the subjects of the stored data. (HIPAA Security Standard)
SECURITY LEVEL DESIGNATION	A rating based on the sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse), and the operational criticality of data processing capabilities (i.e., the consequences where data processing capabilities to be interrupted for some period of time or subjected to fraud or abuse). There are four security level designations for data sensitivity and four security level designations for operational criticality. The highest security level designation for any data or process within an AIS is assigned for the overall security level designation. (DHHS Definition)
SECURITY-RELATED EVENT	An attempt to change the security state of the system (e.g., change discretionary access controls, change the security level of the subject, change user password, etc.). Also included are attempts to violate the security policy of the system (e.g., too many attempts to log on, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file, etc.).
SECURITY SPECIFICATION	A detailed description of the safeguards required to protect a sensitive application [or any AIS asset]. (OMB Circular A-130)
SECURITY VIOLATION	An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources. This includes, but is not limited to, unusual or apparently malicious break-in attempts (either local or over a network), virus or network worm attacks, or file or data tampering, or any incident in which a user, either directly or by using a program, performs unauthorized functions.

TERM	DEFINITION
SENSITIVE APPLICATION	An application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, [or delivery interruption] of the application. (OMB Circular A-130)
SENSITIVE DATA	Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. (OMB Circular A-130)
SENSITIVE INFORMATION	Any information that, if lost, misused, accessed or modified in an improper manner, could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act. (FISCAM) "Sensitive information is any information, of which the loss, misuse, unauthorized access to or modification thereof, could adversely affect the national interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act, the Social Security Act and the Health Insurance Portability and Accountability Act (HIPAA)." (2004 Master Labor Agreement)
SEPARATION OF DUTIES	Separation of duties refers to the policies, procedures, and organizational structure that help ensure one individual cannot independently control all key aspects of a process or computer-related operation. Independent control would enable the individual to conduct unauthorized actions or gain unauthorized access to assets or records without detection. Strict controls involving the maintenance or use of IT assets would ensure that no individual has the ability to both perpetrate and conceal an accidental or intentional breach of IT security.

TERM	DEFINITION
SIGNIFICANT CHANGE	A physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a LAN, changing from batch to on-line processing, adding dial-up capability, and increasing the equipment capacity of the installation. (DHHS Definition)
STANDARDS	Mandatory activities, actions, rules, or regulations designed to provide policies with the support structure and specific direction they require to meaningful and effective.
SYSTEM LIFE CYCLE	The period of time beginning when the software product is conceived and ending when the resultant software products are no longer available for use. The system life cycle is typically broken into phases, such as requirements, design, programming and testing, installation, and operations and maintenance. Each phase consists of a well-defined set of activities whose products lead to the evolution of the activities and products of each successive phase. (FIPS Publication 101)
SYSTEM OWNER/MANAGER	The official who is responsible for the operation and use of an application system. (DHHS Definition)
SYSTEM SECURITY PLAN	A basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. (OMB Bulletin 90-08)
TELECOMMUNICATIONS	A general term for the electronic transmission of information of any type, including data, television pictures, sound, and facsimiles, over any medium such as telephone lines, microwave relay, satellite link, or physical cable. (FISCAM)
THREAT	An entity or event with the potential to harm the system. Typical threats are errors, fraud, disgruntled employees, fires, water damage, hackers, and viruses.
THREAT IDENTIFICATION	The analysis of recognized threats to determine the likelihood of their occurrence and their potential to harm assets.

TERM	DEFINITION
TROJAN HORSE	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. (FISCAM) A destructive program disguised as a game, a utility, or an application. When run, a Trojan horse does something devious to the computer system while appearing to do something useful. (Microsoft Press Computer Dictionary)
USER	The person who uses a computer system and its application programs to perform tasks and produce results. (FISCAM) Any organizational or programmatic entity that [utilizes or] receives service from an [AIS] facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to either the manager or director of the facility or to the same immediate supervisor. (OMB Circular A-130)
VIRUS	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. (FISCAM) A self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating component. (NCSC-TG-004)
VULNERABILITY	A condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat.
WIDE AREA NETWORK (WAN)	A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. (FISCAM) A WAN is a communications network that connects geographically separated areas. (Microsoft Press Computer Dictionary)

TERM	DEFINITION
WORKSTATION	A workstation is a computer built around a single-chip microprocessor. Less powerful than minicomputers and mainframe computers, workstations have nevertheless evolved into very powerful machines capable of complex tasks. Technology is progressing so quickly that state-of-the-art workstations are as powerful as mainframes of only a few years ago, at a fraction of the cost. (Microsoft Press Computer Dictionary)
WORLD-WIDE WEB (WWW or WEB)	The collection of electronic pages, (documents) that are developed in accordance with the HTML (hyper text markup language) Web format standard and may be accessed via Internet connections.
WORM	A worm is a program that propagates itself across computers, usually by spawning copies of itself in each computer's memory. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate segments, a worm is introduced surreptitiously into a host system either for fun or with intent to damage or destroy information. (Microsoft Press Computer Dictionary)